

Red Hat Enterprise Linux 6
Cluster-Administration

Konfiguration und Verwaltung des Hochverfügbarkeits-Add-Ons

Red Hat Enterprise Linux 6 Cluster-Administration

Konfiguration und Verwaltung des Hochverfügbarkeits-Add-Ons

Zusammenfassung

Konfiguration und Verwaltung des Hochverfügbarkeits-Add-Ons beschreibt die Konfiguration und Verwaltung des Hochverfügbarkeits-Add-Ons für Red Hat Enterprise Linux 6.

Inhaltsverzeichnis

Einführung 7
1. Dokumentkonventionen 7
1.1. Typografische Konventionen 7
1.2. Konventionen für Seitenansprachen 9
1.3. Anmerkungen und Warnungen 9
2. Feedback 10

Kapitel 1. Überblick über Konfiguration und Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons 11
1.1. Neue und veränderte Features 11
1.1.1. Neue und veränderte Features für Red Hat Enterprise Linux 6.1 11
1.1.2. Neue und veränderte Features für Red Hat Enterprise Linux 6.2 12
1.1.3. Neue und veränderte Features für Red Hat Enterprise Linux 6.3 13
1.1.4. Neue und veränderte Features für Red Hat Enterprise Linux 6.4 13
1.1.5. Neue und veränderte Features für Red Hat Enterprise Linux 6.5 14
1.2. Konfigurationsgrundlagen 14
1.3. Einrichten der Hardware 15
1.4. Installation der Red Hat Hochverfügbarkeits-Add-On-Software 15

Aktualisieren der Red Hat Hochverfügbarkeits-Add-On-Software 16
1.5. Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software 16

Kapitel 2. Vor der Konfiguration des Hochverfügbarkeits-Add-Ons 18
2.1. Allgemeine Überlegungen zur Konfiguration 18
2.2. Kompatible Hardware 19
2.3. Aktivieren von IP-Ports 20
2.3.1. Aktivieren von IP-Ports auf Cluster-Knoten 20
2.3.2. Aktivieren des IP-Ports für luci 20
2.3.3. Konfiguration der iptables-Firewall zum Erlauben von Cluster-Komponenten 21
2.4. Konfiguration von luci mithilfe von /etc/sysconfig/luci 21
2.5. Konfiguration von ACPI zur Verwendung mit integrierten Fencing-Geräten 22
2.5.1. Deaktivieren von ACPI Soft-Off mit dem chkconfig Befehl 23
2.5.2. Deaktivieren von ACPI Soft-Off im BIOS 24
2.5.3. Vollständiges Deaktivieren von ACPI in der grub.conf Datei 25
2.6. Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten 26
2.7. Überprüfung der Konfiguration 28
2.8. Überlegungen zum NetworkManager 31
2.9. Überlegungen zur Verwendung von Quorum Disk 31
2.10. Red Hat Hochverfügbarkeits-Add-On und SELinux 33
2.11. Multicast-Adressen 33
2.12. UDP-Unicast-Datenverkehr 34
2.13. Überlegungen zu ricci 34
2.14. Konfiguration von virtuellen Maschinen in einer Cluster-Umgebung 34

Kapitel 3. Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Conga 36
3.1. Konfigurationsaufgaben 36
3.2. Starten von luci 36
3.3. Zugriffskontrolle für luci 38
3.4. Erstellen eines Clusters 40
3.5. Globale Cluster-Eigenschaften 42
3.5.1. Konfiguration der allgemeinen Eigenschaften 43
3.5.2. Konfiguration der Fencing-Daemon Eigenschaften 43
3.5.3. Konfiguration des Netzwerks 43

3.5.4. Konfiguration des Redundant Ring Protocols 44
3.5.5. Konfiguration des Quorumdatenträgers 45
3.5.6. Konfiguration der Protokollierung 46
3.6. Konfiguration von Fencing-Geräten 47
3.6.1. Erstellen eines Fencing-Geräts 48
3.6.2. Ändern eines Fencing-Geräts 48
3.6.3. Löschen eines Fencing-Geräts 48
3.7. Konfiguration des Fencings für Cluster-Mitglieder 49
3.7.1. Konfiguration eines einzelnen Fencing-Geräts für einen Knoten 49
3.7.2. Konfiguration eines Backup-Fencing-Geräts 50
3.7.3. Konfiguration eines Knotens mit redundanter Stromversorgung 51
3.8. Konfiguration einer Ausfallsicherungs-Domain 52
3.8.1. Hinzufügen einer Ausfallsicherungs-Domain 53
3.8.2. Ändern einer Ausfallsicherungs-Domain 55
3.8.3. Löschen einer Ausfallsicherungs-Domain 55
3.9. Konfiguration von globalen Cluster-Eigenschaften 55
3.10. Hinzufügen eines Cluster-Dienstes zum Cluster 56

Kapitel 4. Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Conga 59
4.1. Hinzufügen eines vorhandenen Clusters zur luci-Oberfläche 59
4.2. Entfernen eines Clusters aus der luci-Oberfläche 59
4.3. Verwaltung von Cluster-Knoten 60
4.3.1. Einen Cluster-Knoten neu starten 60
4.3.2. Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen 60
4.3.3. Ein Mitglied zu einem laufenden Cluster hinzufügen 61
4.3.4. Ein Mitglied aus einem Cluster löschen 61
4.4. Starten, Stoppen, Neustarten und Löschen von Clustern 62
4.5. Verwaltung von Hochverfügbarkeitsdiensten 63
4.6. Sichern und Wiederherstellen der luci-Konfiguration 64

Kapitel 5. Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit dem ccs Befehl ... 66
5.1. Überblick über operationale Aspekte 66
5.1.1. Erstellen der Cluster-Konfigurationsdatei auf einem lokalen System 67
5.1.2. Anzeigen der aktuellen Cluster-Konfiguration 67
5.1.3. Angeben des ricci-Passworts mit dem ccs-Befehl 67
5.1.4. Ändern von Cluster-Konfigurationskomponenten 68
5.1.5. Befehle, die vorhergehende Einstellungen überschreiben 68
5.1.6. Überprüfung der Konfiguration 69
5.2. Konfigurationsaufgaben 69
5.3. Starten von ricci 69
5.4. Erstellen eines Clusters 70
5.5. Konfigurieren von Fencing-Geräten 71
5.6. Auflisten von Fencing-Geräten und Fencing-Geräteoptionen 73
5.7. Konfigurieren von Fencing-Geräten für Cluster-Mitglieder 75
5.7.1. Konfiguration eines einzelnen Power-Fencing-Geräts für einen Knoten 76
5.7.2. Konfiguration eines einzelnen Speicher-Fencing-Geräts für einen Knoten 77
5.7.3. Konfiguration eines Backup-Fencing-Geräts 79
5.7.4. Konfiguration eines Knotens mit redundanter Stromversorgung 83
5.7.5. Entfernen von Fencing-Methoden und Fencing-Instanzen 85
5.8. Konfigurieren einer Ausfallsicherungs-Domain 86
5.9. Konfigurieren von globalen Cluster-Ressourcen 88
5.10. Hinzufügen eines Cluster-Dienstes zum Cluster 89
5.11. Anzeigen verfügbarer Cluster-Dienste und -Ressourcen 91
5.12. Virtuelle Maschinen-Ressourcen 93
5.13. Konfigurieren eines Quorumdatenträgers 94
5.14. Sonstige Cluster-Konfiguration 96

5.14.1. Cluster-Konfigurationsversion 96
5.14.2. Multicast-Konfiguration 97
5.14.3. Konfiguration eines Zwei-Knoten-Clusters 97
5.14.4. Protokollierung 98
5.14.5. Konfiguration des Redundant Ring Protocols 99
5.15. Verbreiten der Konfigurationsdatei auf den Cluster-Knoten 99

Kapitel 6. Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit ccs **101**
6.1. Verwaltung von Cluster-Knoten 101
6.1.1. Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen 101
6.1.2. Ein Mitglied zu einem laufenden Cluster hinzufügen 101
6.2. Starten und Stoppen eines Clusters 101
6.3. Fehlerdiagnose und -behebung in einem Cluster 102

Kapitel 7. Manuelle Konfiguration von Red Hat Hochverfügbarkeit **103**
7.1. Konfigurationsaufgaben 104
7.2. Erstellen einer einfachen Cluster-Konfigurationsdatei 104

Einfache Konfigurationsbeispiele **106**

Der consensus Wert für totem in einen Zwei-Knoten-Cluster **107**
7.3. Konfiguration von Fencing 108

Fencing-Konfigurationsbeispiele **109**
7.4. Konfiguration von Ausfallsicherungs-Domains 114
7.5. Konfiguration von Hochverfügbarkeitsdiensten 117
7.5.1. Hinzufügen von Cluster-Ressourcen 118
7.5.2. Hinzufügen eines Cluster-Dienstes zum Cluster 120
7.6. Konfiguration von Redundant Ring Protocol 125
7.7. Konfiguration von Debugging-Optionen 126
7.8. Konfiguration von nfsexport- und nfsserver-Ressourcen 126
7.9. Überprüfen der Konfiguration 128

Kapitel 8. Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools . **130**
8.1. Starten und Stoppen der Cluster-Software 130
8.1.1. Starten der Cluster-Software 130
8.1.2. Stoppen der Cluster-Software 131
8.2. Hinzufügen oder Löschen eines Knotens 132
8.2.1. Einen Knoten vom Cluster löschen 132
8.2.2. Einen Knoten zum Cluster hinzufügen 135
8.2.3. Beispiele für Drei-Knoten- und Zwei-Knoten-Konfigurationen 138
8.3. Verwaltung von Hochverfügbarkeitsdiensten 142
8.3.1. Anzeige des Hochverfügbarkeitsdienst-Status mit clustat 142
8.3.2. Verwaltung von Hochverfügbarkeitsdiensten mit clusvcadm 143

Überlegungen zur Verwendung der Freeze- und Unfreeze-Operationen **145**
8.4. Aktualisieren einer Konfiguration 145
8.4.1. Aktualisieren der Konfiguration mittels cman_tool version -r 146
8.4.2. Aktualisieren der Konfiguration mittels scp 147

Kapitel 9. Fehlerdiagnose und -behebung in einem Cluster **149**
9.1. Konfigurationsänderungen werden nicht wirksam 149
9.2. Cluster wird nicht gebildet 150
9.3. Knoten können nach Fencing oder Neustart dem Cluster nicht wieder beitreten 150
9.4. Cluster-Daemon stürzt ab 151
9.4.1. Erstellen eines rgmanager Speicherauszugs zur Laufzeit 151
9.4.2. Erstellen eines Speicherauszugs beim Absturz des Daemons 151

9.4.3. Aufzeichnen einer gdb Backtrace-Sitzung 152
9.5. Cluster-Dienste hängen sich auf 152
9.6. Cluster-Dienst startet nicht 153
9.7. Migration von Cluster-verwalteten Diensten schlägt fehl 153
9.8. Jeder Knoten in einem Zwei-Knoten-Cluster meldet den jeweils anderen Knoten als ausgefallen
9.9. Knoten werden nach LUN-Pfadausfall abgegrenzt 154 154
9.10. Quorumdatenträger erscheint nicht als Cluster-Mitglied 154
9.11. Ungewöhnliches Verhalten bei Ausfallsicherung 154
9.12. Wahlloses Fencing 154
9.13. Debug-Protokollierung für Distributed Lock Manager (DLM) muss aktiviert sein 155

Kapitel 10. SNMP-Konfiguration mit dem Red Hat Hochverfügbarkeits-Add-On 156
10.1. SNMP und das Red Hat Hochverfügbarkeits-Add-On 156
10.2. Konfiguration von SNMP mit dem Red Hat Hochverfügbarkeits-Add-On 156
10.3. Weiterleiten von SNMP-Traps 157
10.4. SNMP-Traps generiert vom Red Hat Hochverfügbarkeits-Add-On 157

Kapitel 11. Konfiguration von geclustertem Samba 159
11.1. Überblick über CTDB 159
11.2. Erforderliche Pakete 159
11.3. GFS2-Konfiguration 159
11.4. CTDB-Konfigurationen 161
11.5. Samba-Konfiguration 163
11.6. Starten von CTDB und Samba-Diensten 164
11.7. Verwenden des geclusterten Samba-Servers 165

Parameter der Fencing-Geräte 166

Parameter der Hochverfügbarkeitsressourcen 192

Verhalten der Hochverfügbarkeitsressourcen 211
C.1. Eltern-, Kind- und Geschwisterrelationen zwischen den Ressourcen 211
C.2. Start-Reihenfolge von Kind- und Geschwisterressourcen 212
C.2.1. Start-/Stopp-Reihenfolge von typisierten Kindressourcen 213

Start-Reihenfolge von typisierten Kindressourcen 214

Stopp-Reihenfolge von typisierten Kindressourcen 214
C.2.2. Start- und Stopp-Reihenfolge von nicht typisierten Kindressourcen 215

Start-Reihenfolge von nicht typisierten Kindressourcen 215

Stopp-Reihenfolge von nicht typisierten Kindressourcen 216
C.3. Vererbung, der <resources> Block, und Wiederverwendung von Ressourcen 216
C.4. Wiederherstellung nach Ausfall und unabhängige Unterbäume 217
C.5. Testen und Fehlerbehebung von Diensten und der Ressourcenreihenfolge 219

Prüfung der Cluster-Dienstressource und Zeitüberschreitung der Ausfallsicherung 221
D.1. Ändern des Intervalls zur Statusprüfung der Ressourcen 221
D.2. Erzwingen von Ressourcen-Timeouts 221

Überblick über Befehlszeilen-Tools 223

High Availability LVM (HA-LVM) 226
F.1. Konfiguration von HA-LVM-Ausfallsicherung mit CLVM (bevorzugt) 227
F.2. Konfiguration von HA-LVM-Ausfallsicherung mit Tagging 228

Versionsgeschichte 230

Stichwortverzeichnis **235**
A 235
B 235
C 235
D 237
E 237
F 237
H 240
I 240
K 240
L 240
M 241
N 241
P 241
Q 241
R 241
S 241
T 242
U 242
V 242
W 242
Z 242

Einführung

Dieses Handbuch liefert Informationen zur Installation, Konfiguration und Verwaltung der Komponenten des Red Hat Hochverfügbarkeits-Add-Ons. Die Komponenten des Red Hat Hochverfügbarkeits-Add-Ons erlauben Ihnen das Verbinden einer Gruppe von Computern (genannt *Knoten* oder *Mitglieder*), um als Cluster zusammenzuarbeiten. In diesem Dokument bezieht sich das Wort *Cluster* auf eine Gruppe von Computern, auf denen das Red Hat Hochverfügbarkeits-Add-On läuft.

Die Zielgruppe dieses Handbuchs sollte bereits über umfassende Kenntnisse von Red Hat Enterprise Linux verfügen und die Grundlagen von Clustern, Speicher und Server-Rechnern verstehen.

Für weitere Informationen über Red Hat Enterprise Linux 6 siehe die folgenden Quellen:

- *Red Hat Enterprise Linux Installationshandbuch* — Liefert Informationen bezüglich der Installation von Red Hat Enterprise Linux 6.
- *Red Hat Enterprise Linux Bereitstellungshandbuch* — Liefert Informationen bezüglich der Implementierung, der Konfiguration und der Administration von Red Hat Enterprise Linux 6.

Für weitere Informationen über das Hochverfügbarkeits-Add-On und zugehörige Produkte für Red Hat Enterprise Linux 6 siehe die folgenden Quellen:

- *Überblick über das Hochverfügbarkeits-Add-On* — Liefert einen umfassenden Überblick über das Red Hat Hochverfügbarkeits-Add-On.
- *Administration des Logical Volume Manager* — Liefert eine Beschreibung des Logical Volume Managers (LVM), inklusive Informationen zum Einsatz von LVM in einer Cluster-Umgebung.
- *Global File System 2: Konfiguration und Administration* — Liefert Informationen zur Installation, Konfiguration und Pflege von Red Hat GFS (Red Hat Global File System 2), das Bestandteil des Resilient Storage Add-Ons ist.
- *DM Multipath* — Liefert Informationen über die Verwendung des Device-Mapper Multi-Pathing-Features von Red Hat Enterprise Linux 6.
- *Lastverteilungs-Administration* — Liefert Informationen zur Konfiguration von Hochleistungssystemen und -diensten mit dem Red Hat Lastverteilungs-Add-On, einer Gruppe integrierter Softwarekomponenten, die Linux Virtual Server (LVS) bereitstellen, um IP-Lasten über eine Gruppe realer Server zu verteilen.
- *Versionshinweise* — Liefert Informationen zu aktuellen Releases von Red Hat Produkten.

Red Hat Cluster Suite Dokumentation und andere Red Hat Dokumente stehen als HTML-, PDF- und RPM-Versionen auf der Red Hat Enterprise Linux Dokumentations-CD und online unter https://access.redhat.com/site/documentation/ zur Verfügung.

1. Dokumentkonventionen

Dieses Handbuch verwendet mehrere Konventionen, um bestimmte Wörter und Sätze hervorzuheben und Aufmerksamkeit auf bestimmte Informationen zu lenken.

In PDF- und Papierausgaben verwendet dieses Handbuch Schriftbilder des Liberation-Fonts-Sets. Das Liberation-Fonts-Set wird auch für HTML-Ausgaben verwendet, falls es auf Ihrem System installiert ist. Falls nicht, werden alternative, aber äquivalente Schriftbilder angezeigt. Beachten Sie: Red Hat Enterprise Linux 5 und die nachfolgende Versionen beinhalten das Liberation-Fonts-Set standardmäßig.

1.1. Typografische Konventionen

Es werden vier typografische Konventionen verwendet, um die Aufmerksamkeit auf bestimmte Wörter und Sätze zu lenken. Diese Konventionen und die Umstände, unter denen sie auftreten, sind folgende:

`Nichtproportional Fett`

Dies wird verwendet, um Systemeingaben hervorzuheben, einschließlich Shell-Befehle, Dateinamen und -pfade. Es wird ebenfalls zum Hervorheben von Tasten und Tastenkombinationen verwendet. Zum

Beispiel:

> Um den Inhalt der Datei **`my_next_bestselling_novel`** in Ihrem aktuellen Arbeitsverzeichnis zu sehen, geben Sie den Befehl **`cat my_next_bestselling_novel`** in den Shell-Prompt ein und drücken Sie **`Enter`**, um den Befehl auszuführen.

Das oben aufgeführte Beispiel beinhaltet einen Dateinamen, einen Shell-Befehl und eine Taste. Alle werden nichtproportional fett dargestellt und alle können, dank des Kontextes, leicht unterschieden werden.

Tastenkombinationen unterscheiden sich von einzelnen Tasten durch das Pluszeichen, das die einzelnen Teile einer Tastenkombination miteinander verbindet. Zum Beispiel:

> Drücken Sie **`Enter`**, um den Befehl auszuführen.
>
> Drücken Sie **`Strg`**+**`Alt`**+**`F2`**, um zu einem virtuellen Terminal zu wechseln.

Das erste Beispiel hebt die zu drückende Taste hervor. Das zweite Beispiel hebt eine Tastenkombination hervor: eine Gruppe von drei Tasten, die gleichzeitig gedrückt werden müssen.

Falls Quellcode diskutiert wird, werden Klassennamen, Methoden, Funktionen, Variablennamen und Rückgabewerte, die innerhalb eines Abschnitts erwähnt werden, wie oben gezeigt **`nichtproportional fett`** dargestellt. Zum Beispiel:

> Zu dateiverwandten Klassen zählen **`filesystem`** für Dateisysteme, **`file`** für Dateien und **`dir`** für Verzeichnisse. Jede Klasse hat ihren eigenen Satz an Berechtigungen.

Proportional Fett

Dies kennzeichnet Wörter oder Sätze, die auf einem System vorkommen, einschließlich Applikationsnamen, Text in Dialogfeldern, beschriftete Schaltflächen, Bezeichnungen für Auswahlkästchen und Radio-Buttons, Überschriften von Menüs und Untermenüs. Zum Beispiel:

> Wählen Sie **System** → **Einstellungen** → **Maus** in der Hauptmenüleiste aus, um die **Mauseinstellungen** zu öffnen. Wählen Sie im Reiter **`Tasten`** auf das Auswahlkästchen **`Mit links bediente Maus`** und anschließend auf **`Schließen`**, um die primäre Maustaste von der linken auf die rechte Seite zu ändern (d.h., um die Maus auf Linkshänder anzupassen).
>
> Um ein Sonderzeichen in eine **gedit**-Datei einzufügen, wählen Sie **Anwendungen** → **Zubehör** → **Zeichentabelle** aus der Hauptmenüleiste. Wählen Sie als Nächstes **Suchen** → **Suchen** aus der Menüleiste der **Zeichentabelle**, geben Sie im Feld **`Suchbegriff`** den Namen des Zeichens ein und klicken Sie auf **`Weitersuchen`**. Das gesuchte Zeichen wird daraufhin in der **`Zeichentabelle`** hervorgehoben. Doppelklicken Sie auf dieses hervorgehobene Zeichen, um es in das Feld **`Zu kopierender Text`** zu übernehmen und klicken Sie anschließend auf die Schaltfläche **`Kopieren`**. Gehen Sie nun zurück in Ihr Dokument und wählen Sie **Bearbeiten** → **Einfügen** aus der **gedit**-Menüleiste.

Der oben aufgeführte Text enthält Applikationsnamen, systemweite Menünamen und -elemente, applikationsspezifische Menünamen sowie Schaltflächen und Text innerhalb einer grafischen Oberfläche. Alle werden proportional fett dargestellt und sind anhand des Kontextes unterscheidbar.

`Nichtproportional Fett Kursiv` oder ***`Proportional Fett Kursiv`***

Sowohl bei nichtproportional fett als auch bei proportional fett weist ein zusätzlicher Kursivdruck auf einen ersetzbaren oder variablen Text hin. Kursivdruck kennzeichnet Text, der nicht wörtlich eingeben wird, oder angezeigten Text, der sich abhängig von den gegebenen Umständen unterscheiden kann. Zum Beispiel:

> Um sich mit einer Remote-Maschine via SSH zu verbinden, geben Sie an einem Shell-

Prompt **ssh *username@domain.name*** ein. Falls die Remote-Maschine **example.com** ist und Ihr Benutzername auf dieser Maschine John lautet, geben Sie also **ssh john@example.com** ein.

Der Befehl **mount -o remount *file-system*** hängt das angegebene Dateisystem wieder ein. Um beispielsweise das **/home**-Dateisystem wieder einzuhängen, verwenden Sie den Befehl **mount -o remount /home**.

Um die Version des derzeit installierten Pakets zu sehen, verwenden Sie den Befehl **rpm -q *package***. Die Ausgabe sieht wie folgt aus: ***package-version-release***.

Beachten Sie die kursiv dargestellten Begriffe oben — username, domain.name, file-system, package, version und release. Jedes Wort ist ein Platzhalter entweder für Text, den Sie für einen Befehl eingeben, oder für Text, der vom System angezeigt wird.

Neben der Standardbenutzung für die Darstellung des Titels eines Werks zeigt der Kursivdruck auch die erstmalige Verwendung eines neuen und wichtigen Begriffs an. Zum Beispiel:

Publican ist ein *DocBook* Publishing-System.

1.2. Konventionen für Seitenansprachen

Ausgaben des Terminals und Auszüge aus dem Quellcode werden visuell vom umliegenden Text hervorgehoben durch sogenannte Seitenansprachen (auch Pull-Quotes genannt).

Eine an das Terminal gesendete Ausgabe wird in den Schrifttyp **nichtproportional Roman** gesetzt und wie folgt dargestellt:

```
books        Desktop   documentation  drafts  mss    photos   stuff  svn
books_tests  Desktop1  downloads      images  notes  scripts  svgs
```

Auszüge aus dem Quellcode werden ebenfalls in den Schrifttyp **nichtproportional Roman** gesetzt, doch wird zusätzlich noch die Syntax hervorgehoben:

```
static int kvm_vm_ioctl_deassign_device(struct kvm *kvm,
                 struct kvm_assigned_pci_dev *assigned_dev)
{
         int r = 0;
         struct kvm_assigned_dev_kernel *match;

         mutex_lock(&kvm->lock);

         match = kvm_find_assigned_dev(&kvm->arch.assigned_dev_head,
                                       assigned_dev->assigned_dev_id);
         if (!match) {
                 printk(KERN_INFO "%s: device hasn't been assigned before, "
                   "so cannot be deassigned\n", __func__);
                 r = -EINVAL;
                 goto out;
         }

         kvm_deassign_device(kvm, match);

         kvm_free_assigned_device(kvm, match);

out:
         mutex_unlock(&kvm->lock);
         return r;
}
```

1.3. Anmerkungen und Warnungen

Zu guter Letzt verwenden wir drei visuelle Stile, um die Aufmerksamkeit auf Informationen zu lenken, die andernfalls vielleicht übersehen werden könnten.



Anmerkung

Eine Anmerkung ist ein Tipp, ein abgekürztes Verfahren oder ein alternativer Ansatz für die vorliegende Aufgabe. Das Ignorieren von Anmerkungen sollte keine negativen Auswirkungen haben, aber Sie verpassen so vielleicht einen Trick, der Ihnen das Leben vereinfachen könnte.



Wichtig

Die Wichtig-Schaukästen lenken die Aufmerksamkeit auf Dinge, die sonst leicht übersehen werden können: Konfigurationsänderungen, die nur für die aktuelle Sitzung gelten oder Dienste, für die ein Neustart nötig ist, bevor eine Aktualisierung wirksam wird. Das Ignorieren von Wichtig-Schaukästen würde keinen Datenverlust verursachen, kann aber unter Umständen zu Ärgernissen und Frustration führen.



Warnung

Eine Warnung sollte nicht ignoriert werden. Das Ignorieren von Warnungen führt mit hoher Wahrscheinlichkeit zu Datenverlust.

2. Feedback

Falls Sie einen Fehler in diesem Handbuch finden oder eine Idee haben, wie dieses verbessert werden könnte, freuen wir uns über Ihr Feedback! Bitte reichen Sie einen Bericht in Bugzilla ein: http://bugzilla.redhat.com/bugzilla/. Reichen Sie den Fehlerbericht für das Produkt **Red Hat Enterprise Linux 6** und die Komponente **doc-Cluster_Administration** ein.

Vergewissern Sie sich beim Einreichen eines Fehlerberichts, dass Sie die Kennung des Handbuchs mit angeben:

```
Cluster_Administration(EN)-6 (2013-11-13T16:26)
```

Indem Sie die Kennung des Handbuchs angeben, wissen wir genau, welche Version des Handbuchs Sie vorliegen haben.

Falls Sie uns einen Vorschlag zur Verbesserung der Dokumentation senden möchten, sollten Sie hierzu möglichst genaue Angaben machen. Wenn Sie einen Fehler gefunden haben, geben Sie bitte die Nummer des Abschnitts und einen Ausschnitt des Textes an, damit wir diesen leicht finden können.

Kapitel 1. Überblick über Konfiguration und Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons

Das Red Hat Hochverfügbarkeits-Add-On erlaubt Ihnen das Verbinden einer Gruppe von Computern (genannt *Knoten* oder *Mitglieder*), um als Cluster zusammenzuarbeiten. Sie können das Red Hat Hochverfügbarkeits-Add-On auf Ihre Clustering-Bedürfnisse anpassen (z.B. zum Einrichten eines Clusters zur gemeinsamen Dateinutzung auf einem GFS2-Dateisystem oder zum Einrichten einer Dienstausfallsicherung).



Anmerkung

Informationen über bewährte Verfahren zur Bereitstellung und Aktualisierung von Red Hat Enterprise Linux Clustern unter Verwendung des Hochverfügbarkeits-Add-Ons und Red Hat Global File System 2 (GFS2) finden Sie im Artikel "Red Hat Enterprise Linux Cluster, High Availability, and GFS Deployment Best Practices" im Red Hat Kundenportal unter https://access.redhat.com/site/articles/40051.

Dieses Kapitel liefert eine Zusammenfassung der Features und Aktualisierungen, die seit der ursprünglichen Release von Red Hat Enterprise Linux 6 zum Red Hat Hochverfügbarkeits-Add-On hinzugefügt wurden, gefolgt von einer Übersicht über die Konfiguration und Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons.

1.1. Neue und veränderte Features

Dieser Abschnitt führt die Features und Aktualisierungen an, die seit der ursprünglichen Release von Red Hat Enterprise Linux 6 zum Red Hat Hochverfügbarkeits-Add-On hinzugefügt wurden.

1.1.1. Neue und veränderte Features für Red Hat Enterprise Linux 6.1

Red Hat Enterprise Linux 6.1 führt die folgenden Änderungen und Aktualisierungen an Dokumentationen und Features ein.

- Ab der Red Hat Enterprise Linux 6.1 Release bietet das Red Hat Hochverfügbarkeits-Add-On Unterstützung für SNMP-Traps. Informationen über die Konfiguration von SNMP-Traps mit dem Red Hat Hochverfügbarkeits-Add-On finden Sie in Kapitel 10, *SNMP-Konfiguration mit dem Red Hat Hochverfügbarkeits-Add-On*.
- Ab der Red Hat Enterprise Linux 6.1 Release bietet das Red Hat Hochverfügbarkeits-Add-On Unterstützung für den **ccs** Cluster-Konfigurationsbefehl. Informationen über den **ccs** Befehl finden Sie in Kapitel 5, *Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit dem **ccs** Befehl* und Kapitel 6, *Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit **ccs***.
- Die Dokumentation über die Konfiguration und Verwaltung der Red Hat Hochverfügbarkeits-Add-On-Software mittels Conga wurde aktualisiert, um aktuelle Conga-Oberflächen und unterstützte Features aufzunehmen.
- Für die Red Hat Enterprise Linux 6.1 Release und später ist für die Verwendung von **ricci** ein Passwort erforderlich, wenn Sie zum ersten Mal eine aktualisierte Cluster-Konfiguration von einem bestimmten Knoten verbreiten. Weitere Informationen über **ricci** finden Sie unter Abschnitt 2.13, „Überlegungen zu **ricci**“.
- Sie können nun die *Restart-Disable* Wiederherstellungsrichtlinie für einen Dienst festlegen, wodurch das System einen Neustart des ausgefallenen Dienstes an demselben Standort versucht. Scheitert dieser Versuch, wird der Dienst deaktiviert, statt auf einen anderen Host im Cluster verlegt zu werden. Dieses Feature ist in Abschnitt 3.10, „Hinzufügen eines Cluster-Dienstes zum Cluster“ und Anhang B, *Parameter der Hochverfügbarkeitsressourcen* dokumentiert.
- Sie können nun einen unabhängigen Unterbaum als nicht-kritisch konfigurieren, so dass im Falle eines Ausfalls dieser Ressource nur diese Ressource deaktiviert wird (statt des gesamten Dienstes). Informationen über dieses Feature finden Sie in Abschnitt 3.10, „Hinzufügen eines

Cluster-Dienstes zum Cluster“ und Abschnitt C.4, „Wiederherstellung nach Ausfall und unabhängige Unterbäume“.
- Dieses Dokument enthält nun das neue Kapitel Kapitel 9, *Fehlerdiagnose und -behebung in einem Cluster*.

Zusätzlich wurden im gesamten Dokument kleinere Korrekturen vorgenommen und einige Sachverhalte verdeutlicht.

1.1.2. Neue und veränderte Features für Red Hat Enterprise Linux 6.2

Red Hat Enterprise Linux 6.2 führt die folgenden Änderungen und Aktualisierungen an Dokumentationen und Features ein.

- Red Hat Enterprise Linux bietet nun Unterstützung für den Einsatz von geclustertem Samba in einer active/active-Konfiguration. Für Informationen über die Konfiguration von geclustertem Samba siehe Kapitel 11, *Konfiguration von geclustertem Samba*.
- Jeder Benutzer, der sich auf dem System anmelden kann, das **luci** hostet, kann sich auch bei **luci** anmelden. Ab Red Hat Enterprise Linux 6.2 jedoch kann nur der Root-Benutzer auf dem System, das **luci** ausführt, auf die **luci** Komponenten zugreifen, bis ein Administrator (der Root-Benutzer oder ein anderer Benutzer mit Administratorrechten) die Berechtigungen für diesen Benutzer erstellt. Für Informationen über das Erstellen von **luci** Berechtigungen für Benutzer siehe Abschnitt 3.3, „Zugriffskontrolle für luci“.
- Die Knoten in einem Cluster können miteinander über den UDP-Unicast-Transportmechanismus kommunizieren. Weitere Informationen zur Konfiguration von UDP-Unicast siehe Abschnitt 2.12, „UDP-Unicast-Datenverkehr“.
- Sie können nun einige Aspekte von **luci**s Verhalten mithilfe der **/etc/sysconfig/luci** Datei konfigurieren. Beispielsweise können Sie speziell festlegen, auf welcher IP-Adresse **luci** bereitgestellt werden soll. Weitere Informationen über das Konfigurieren der IP-Adresse, auf der **luci** bereitgestellt wird, finden Sie in Tabelle 2.2, „Aktivierter IP-Port auf einem Computer, der luci ausführt“. Allgemeine Informationen über die **/etc/sysconfig/luci** Datei finden Sie in Abschnitt 2.4, „Konfiguration von **luci** mithilfe von **/etc/sysconfig/luci**“.
- Der **ccs** Befehl beinhaltet nun die **--lsfenceopts** Option, die eine Liste der verfügbaren Fencing-Geräte ausgibt, sowie die **--lsfenceopts** ***fence_type*** Option, die jeden verfügbaren Fencing-Typ ausgibt. Für Informationen über diese Optionen siehe Abschnitt 5.6, „Auflisten von Fencing-Geräten und Fencing-Geräteoptionen“.
- Der **ccs** Befehl beinhaltet nun die Option **--lsserviceopts**, die eine Liste der für Ihren Cluster verfügbaren Cluster-Dienste ausgibt, sowie die Option **--lsserviceopts** ***service_type***, die eine Liste der Optionen ausgibt, die Sie für einen bestimmten Diensttyp spezifizieren können. Informationen über diese Optionen finden Sie in Abschnitt 5.11, „Anzeigen verfügbarer Cluster-Dienste und -Ressourcen“.
- Die Red Hat Enterprise Linux 6.2 Release bietet Unterstützung für den VMware Fencing-Agenten (SOAP-Schnittstelle). Informationen über Fencing-Geräteparameter finden Sie unter Anhang A, *Parameter der Fencing-Geräte*.
- Die Red Hat Enterprise Linux 6.2 Release bietet Unterstützung für den RHEV-M REST API Fencing-Agenten mit RHEV 3.0 und höher. Informationen über Fencing-Geräteparameter finden Sie unter Anhang A, *Parameter der Fencing-Geräte*.
- Ab der Red Hat Enterprise Linux 6.2 Release können Sie bei der Konfiguration einer virtuellen Maschine in einem Cluster mit dem **ccs** Befehl die Option **--addvm** verwenden (statt der **addservice** Option). Dadurch wird gewährleistet, dass die **vm** Ressource direkt unter dem **rm** Konfigurationsknoten in der Cluster-Konfigurationsdatei definiert wird. Informationen über die Konfiguration von virtuellen Maschinen-Ressourcen mit dem **ccs** Befehl finden Sie in Abschnitt 5.12, „Virtuelle Maschinen-Ressourcen“.
- Dieses Dokument enthält einen neuen Anhang, Anhang D, *Prüfung der Cluster-Dienstressource und Zeitüberschreitung der Ausfallsicherung*. Dieser Anhang beschreibt, wie **rgmanager** den Status von Cluster-Ressourcen überwacht und wie die Zeitabstände der Statusprüfungen verändert werden können. Der Anhang beschreibt außerdem den **__enforce_timeouts** Dienstparameter, der

festlegt, dass eine Zeitüberschreitung für eine Operation zum Fehlschlagen des Dienstes führen soll.

- Dieses Dokument enthält einen neuen Abschnitt, Abschnitt 2.3.3, „Konfiguration der iptables-Firewall zum Erlauben von Cluster-Komponenten“. Dieser Abschnitt zeigt die Filterung, die Sie verwenden können, um Multicast-Datenverkehr durch die **iptables** Firewall für die verschiedenen Cluster-Komponenten zu ermöglichen.

Zusätzlich wurden im gesamten Dokument kleinere Korrekturen vorgenommen und einige Sachverhalte verdeutlicht.

1.1.3. Neue und veränderte Features für Red Hat Enterprise Linux 6.3

Red Hat Enterprise Linux 6.3 führt die folgenden Änderungen und Aktualisierungen an Dokumentationen und Features ein.

- Die Red Hat Enterprise Linux 6.3 Release bietet Unterstützung für den **condor** Ressourcen-Agent. Für Informationen über HA-Ressourcenparameter siehe Anhang B, *Parameter der Hochverfügbarkeitsressourcen*.
- Dieses Dokument enthält einen neuen Anhang, Anhang F, *High Availability LVM (HA-LVM)*.
- Sämtliche Anleitungen in diesem Dokument heben nun deutlicher hervor, welche Konfigurationsänderungen einen Cluster-Neustart erfordern. Eine Übersicht dieser Änderungen finden Sie in Abschnitt 9.1, „Konfigurationsänderungen werden nicht wirksam“.
- Die Dokumentation weist nun darauf hin, dass es eine automatische Abmeldung gibt, die Sie nach 15 Minuten Inaktivität aus **luci** abmeldet. Für Information zum Start von **luci** siehe Abschnitt 3.2, „Starten von **luci** “.
- Das **fence_ipmilan** Fencing-Gerät unterstützt einen Parameter für Berechtigungsebenen. Für Informationen über Fencing-Geräteparameter siehe Anhang A, *Parameter der Fencing-Geräte*.
- Dieses Dokument enthält einen neuen Abschnitt, Abschnitt 2.14, „Konfiguration von virtuellen Maschinen in einer Cluster-Umgebung“.
- Dieses Dokument enthält einen neuen Abschnitt, Abschnitt 4.6, „Sichern und Wiederherstellen der luci-Konfiguration“.
- Dieses Dokument enthält einen neuen Abschnitt, Abschnitt 9.4, „Cluster-Daemon stürzt ab“.
- Dieses Dokument enthält Informationen über das Erstellen von Debug-Optionen in Abschnitt 5.14.4, „Protokollierung“, Abschnitt 7.7, „Konfiguration von Debugging-Optionen“ und Abschnitt 9.13, „Debug-Protokollierung für Distributed Lock Manager (DLM) muss aktiviert sein“.
- Ab Red Hat Enterprise Linux 6.3 kann der Root-Benutzer oder ein Benutzer mit **luci** Administratorrechten auch die **luci** Oberfläche nutzen, um Benutzer zum System hinzuzufügen, wie in Abschnitt 3.3, „Zugriffskontrolle für luci“ beschrieben.
- Ab der Red Hat Enterprise Linux 6.3 Release prüft der **ccs** Befehl die Konfiguration anhand des Cluster-Schemas unter **/usr/share/cluster/cluster.rng** auf demjenigen Knoten, den Sie mithilfe der **-h** Option spezifizieren. Bislang verwendete der **ccs** Befehl stets das Cluster-Schema, das im **ccs** Befehl integriert war, also **/usr/share/ccs/cluster.rng** auf dem lokalen System. Informationen über die Konfigurationsprüfung finden Sie in Abschnitt 5.1.6, „Überprüfung der Konfiguration“.
- Die Tabellen der Fencing-Geräteparameter in Anhang A, *Parameter der Fencing-Geräte* und die Tabellen der HA-Ressourcenparameter in Anhang B, *Parameter der Hochverfügbarkeitsressourcen* enthalten nun die Namen der Parameter, wie sie in der **cluster.conf** Datei auftreten.

Zusätzlich wurden im gesamten Dokument kleinere Korrekturen vorgenommen und einige Sachverhalte verdeutlicht.

1.1.4. Neue und veränderte Features für Red Hat Enterprise Linux 6.4

Red Hat Enterprise Linux 6.4 führt die folgenden Änderungen und Aktualisierungen an Dokumentationen und Features ein.

- Die Red Hat Enterprise Linux 6.4 Release bietet Unterstützung für den Eaton Network Power

Controller (SNMP Interface) Fencing-Agenten, den HP BladeSystem Fencing-Agenten, und den IBM iPDU Fencing-Agenten. Informationen über Fencing-Geräteparameter finden Sie unter Anhang A, *Parameter der Fencing-Geräte*.

- Anhang B, *Parameter der Hochverfügbarkeitsressourcen* bietet nun eine Beschreibung des NFS-Server Ressourcen-Agenten
- Ab Red Hat Enterprise Linux 6.3 kann der Root-Benutzer oder ein Benutzer mit **luci** Administratorrechten auch die **luci** Oberfläche nutzen, um Benutzer vom System zu entfernen. Dieses ist dokumentiert in Abschnitt 3.3, „Zugriffskontrolle für luci“.
- Anhang B, *Parameter der Hochverfügbarkeitsressourcen* enthält eine Beschreibung des neuen **nfsrestart** Parameters für die Dateisystem und GFS2 HA Ressourcen.
- Dieses Dokument enthält einen neuen Abschnitt, Abschnitt 5.1.5, „Befehle, die vorhergehende Einstellungen überschreiben“.
- Abschnitt 2.3, „Aktivieren von IP-Ports“ enthält nun Informationen über das Filtern der **iptables** Firewall für **igmp**.
- Der IPMI LAN Fencing-Agent unterstützt jetzt einen Parameter, um die Berechtigungsstufe auf dem IPMI-Gerät zu konfigurieren, wie in Anhang A, *Parameter der Fencing-Geräte* dokumentiert.
- Neben dem Ethernet Bonding-Modus 1 werden jetzt auch Bonding-Modus 0 und 2 für die Kommunikation zwischen Knoten in einem Cluster unterstützt. Die Ratschläge in diesem Dokument zur Suche und Bereinigung von Fehlern, die darauf hinweisen, nur unterstützte Bonding-Modi zu verwenden, wurden entsprechend angepasst.
- VLAN-markierte Netzwerkgeräte werden jetzt für Cluster-Heartbeat-Kommunikation unterstützt. Die Ratschläge zur Suche und Bereinigung von Fehlern, die darauf hinweisen, dass dies nicht unterstützt wird, wurden aus diesem Dokument entfernt.
- Das Red Hat Hochverfügbarkeits-Add-On unterstützt jetzt die Konfiguration des Redundant Ring Protocolss. Für allgemeine Informationen zur Verwendung dieser Funktion und Konfiguration der **cluster.conf** Konfigurationsdatei siehe Abschnitt 7.6, „Konfiguration von Redundant Ring Protocol“. Für weitere Informationen zur Konfiguration des Redundant Ring Protocolss mit **luci** siehe Abschnitt 3.5.4, „Konfiguration des Redundant Ring Protocols“. Für weitere Informationen zur Konfiguration des Redundant Ring Protocolss mit dem **ccs** Befehl siehe Abschnitt 5.14.5, „Konfiguration des Redundant Ring Protocols“.

Zusätzlich wurden im gesamten Dokument kleinere Korrekturen vorgenommen und einige Sachverhalte verdeutlicht.

1.1.5. Neue und veränderte Features für Red Hat Enterprise Linux 6.5

Red Hat Enterprise Linux 6.5 führt die folgenden Änderungen und Aktualisierungen an Dokumentationen und Features ein.

- Dieses Dokument enthält einen neuen Abschnitt, Abschnitt 7.8, „Konfiguration von nfsexport- und nfsserver-Ressourcen“.
- Die Tabellen der Fencing-Geräteparameter in Anhang A, *Parameter der Fencing-Geräte* wurden aktualisiert, um kleine Änderungen an der **luci** Oberfläche widerzuspiegeln.

Zusätzlich wurden im gesamten Dokument viele kleinere Korrekturen vorgenommen und einige Sachverhalte verdeutlicht.

1.2. Konfigurationsgrundlagen

Um einen Cluster einzurichten, müssen Sie die Knoten an bestimmte Cluster-Hardware anschließen und die Knoten für die Cluster-Umgebung konfigurieren. Die Konfiguration und Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons umfasst die folgenden, grundlegenden Schritte:

1. Einrichten der Hardware. Siehe Abschnitt 1.3, „Einrichten der Hardware“.
2. Installation der Red Hat Hochverfügbarkeits-Add-On Software. Siehe Abschnitt 1.4, „Installation der Red Hat Hochverfügbarkeits-Add-On-Software“.

3. Konfiguration der Red Hat Hochverfügbarkeits-Add-On Software. Siehe Abschnitt 1.5, „Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software“.

1.3. Einrichten der Hardware

Zum Einrichten der Hardware gehört das Verbinden der Cluster-Knoten mit anderer Hardware, die zum Ausführen des Red Hat Hochverfügbarkeits-Add-Ons nötig ist. Der Umfang und die Art der Hardware richtet sich nach dem Zweck und den Ansprüchen an die Verfügbarkeit des Clusters. In der Regel erfordert ein Cluster auf Unternehmensebene die folgende Hardware (siehe Abbildung 1.1, „Überblick über die Red Hat Hochverfügbarkeits-Add-On-Hardware“). Für Hardware-Überlegungen und andere Themen der Cluster-Konfiguration siehe Kapitel 2, *Vor der Konfiguration des Hochverfügbarkeits-Add-Ons* oder setzen Sie sich mit einem autorisierten Red Hat Vertreter in Verbindung.

- Cluster-Knoten — Computer, die in der Lage sind Red Hat Enterprise Linux 6 Software durchzuführen, mit mindestens 1 GB RAM.
- Netzwerk-Switches für öffentliches Netzwerk — Dies ist nötig für den Client-Zugriff auf den Cluster.
- Netzwerk-Switches für privates Netzwerk — Dies ist nötig zur Kommunikation zwischen den Cluster-Knoten und anderer Cluster-Hardware wie z.B. Network Power Switches und Fibre Channel Switches.
- Fencing-Gerät — Ein Fencing-Gerät ist erforderlich. Ein Network Power Switch wird empfohlen, um Fencing in einem Cluster auf Unternehmensebene durchzuführen. Informationen über unterstützte Fencing-Geräte finden Sie in Anhang A, *Parameter der Fencing-Geräte*.
- Speicher — Für einen Cluster benötigen Sie Speicherplatz. Abbildung 1.1, „Überblick über die Red Hat Hochverfügbarkeits-Add-On-Hardware“ zeigt gemeinsam verwendeten Speicher, doch für Ihre Anforderungen ist gemeinsam verwendeter Speicher gegebenenfalls nicht erforderlich.

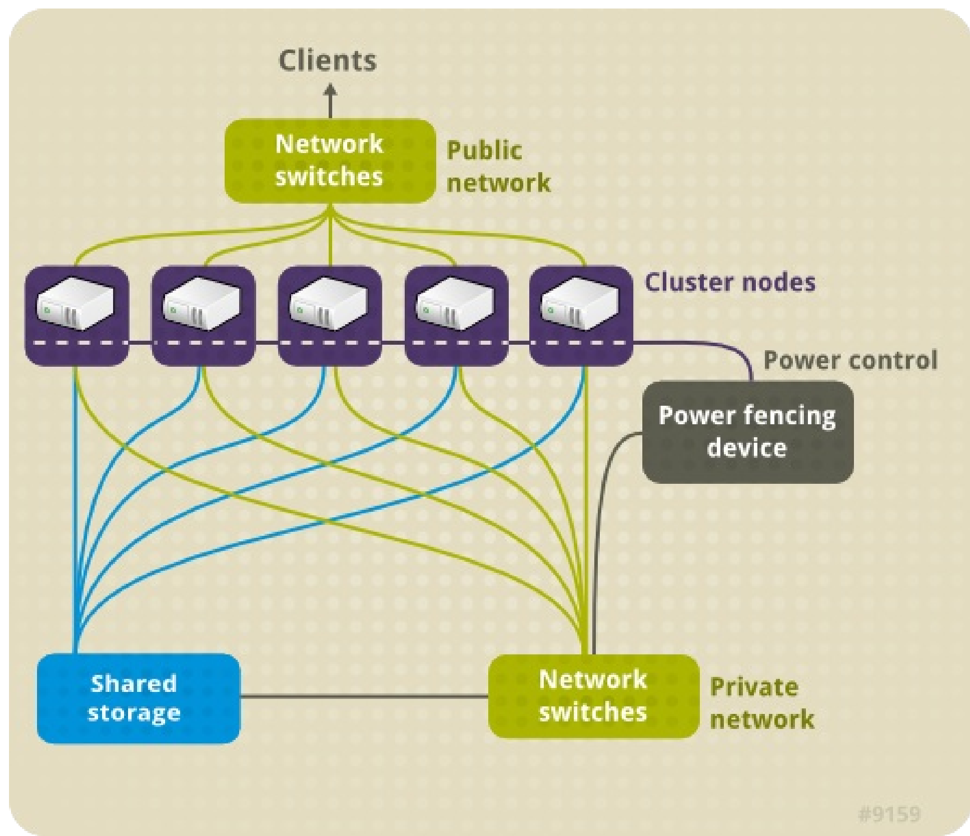


Abbildung 1.1. Überblick über die Red Hat Hochverfügbarkeits-Add-On-Hardware

1.4. Installation der Red Hat Hochverfügbarkeits-Add-On-Software

Um Red Hat High Availability-Add-On-Software zu installieren, müssen Sie Berechtigungen für die Software haben. Wenn Sie das **luci** Konfigurations-GUI verwenden, können Sie damit die Cluster-Software installieren. Wenn Sie andere Werkzeuge verwenden, um den Cluster zu konfigurieren, sichern und installieren Sie die Software, wie Sie es auch mit der Red Hat Enterprise Linux Software tun würden.

Sie können den folgenden **`yum install`** Befehl verwenden, um die Red Hat Hochverfügbarkeits-Add-On-Software-Pakete zu installieren:

```
# yum install rgmanager lvm2-cluster gfs2-utils
```

Beachten Sie, dass bei Installation des **`rgmanager`** alle notwendigen Abhängigkeiten, um einen HA-Cluster aus dem HighAvailability-Channel zu erstellen, eingeschlossen werden. Die **`lvm2-cluster`** und **`gfs2-utils`** Pakete sind Teil des ResilientStorage-Channels und werden für Ihren Cluster ggf. nicht benötigt.

Aktualisieren der Red Hat Hochverfügbarkeits-Add-On-Software

Es ist möglich, die Cluster-Software auf eine beliebige Hauptversion von Red Hat Enterprise Linux zu aktualisieren, ohne den Cluster dafür außer Betrieb nehmen zu müssen. Dafür muss die Cluster-Software auf allen Hosts einzeln nacheinander deaktiviert, die Software aktualisiert und anschließend die Cluster-Software auf dem Host wieder gestartet werden.

1. Halten Sie sämtliche Cluster-Dienste auf einem einzelnen Cluster-Knoten an. Eine Anleitung zum Stoppen der Cluster-Software auf einem Knoten finden Sie in Abschnitt 8.1.2, „Stoppen der Cluster-Software“. Gegebenenfalls kann es von Vorteil sein, cluster-verwaltete Dienste und virtuelle Maschinen manuell vom Host zu verlegen, bevor **`rgmanager`** gestoppt wird.
2. Führen Sie den **`yum update`** Befehl durch, um die installierten Pakete zu aktualisieren.
3. Starten Sie den Cluster-Knoten neu oder führen Sie manuell einen Neustart der Cluster-Dienste aus. Eine Anleitung zum Starten der Cluster-Software auf einem Knoten finden Sie in Abschnitt 8.1.1, „Starten der Cluster-Software“.

1.5. Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software

Zur Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software gehört die Verwendung von Konfigurations-Tools, um die Relationen der Cluster-Komponenten untereinander zu definieren. Die folgenden Cluster-Konfigurations-Tools stehen im Rahmen des Red Hat Hochverfügbarkeits-Add-Ons zur Verfügung:

- **Conga** — Hierbei handelt es sich um eine umfangreiche Benutzeroberfläche zur Installation, Konfiguration und Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons. Siehe Kapitel 3, *Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit **Conga*** und Kapitel 4, *Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit **Conga*** für Informationen zur Konfiguration und Verwaltung des Hochverfügbarkeits-Add-Ons mit **Conga** .
- Der **`ccs`** Befehl — Dieser Befehl konfiguriert und verwaltet das Red Hat Hochverfügbarkeits-Add-On. Siehe Kapitel 5, *Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit dem **ccs** Befehl* und Kapitel 6, *Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit **ccs*** für Informationen zur Konfiguration und Verwaltung des Hochverfügbarkeits-Add-Ons mit dem **`ccs`** Befehl.
- Befehlszeilen-Tools — Hierbei handelt es sich um eine Reihe von Befehlszeilen-Tools zur Konfiguration und Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons. Siehe Kapitel 7, *Manuelle Konfiguration von Red Hat Hochverfügbarkeit* und Kapitel 8, *Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools* für Informationen zur Konfiguration und Verwaltung eines Clusters mit Befehlszeilen-Tools. Siehe Anhang E, *Überblick über Befehlszeilen-Tools* für eine Übersicht der bevorzugten Befehlszeilen-Tools.



Anmerkung

`system-config-cluster` steht in Red Hat Enterprise Linux 6 nicht zur Verfügung.

Kapitel 2. Vor der Konfiguration des Hochverfügbarkeits-Add-Ons

Dieses Kapitel beschreibt die Aufgaben, die vor der Installation und Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons durchgeführt werden müssen. Es besteht aus den folgenden Abschnitten.



Wichtig

Stellen Sie sicher, dass Ihre Bereitstellung des Red Hat Hochverfügbarkeits-Add-Ons Ihren Anforderungen gerecht wird und unterstützt werden kann. Beratschlagen Sie sich dazu ggf. mit einem autorisierten Red Hat Vertreter, um Ihre Konfiguration vor der Bereitstellung zu prüfen. Berücksichtigen Sie zudem eine gewisse Zeit für einen Burn-In-Test, um die Konfiguration auf mögliche Ausfälle zu überprüfen.

- Abschnitt 2.1, „Allgemeine Überlegungen zur Konfiguration“
- Abschnitt 2.2, „Kompatible Hardware“
- Abschnitt 2.3, „Aktivieren von IP-Ports“
- Abschnitt 2.4, „Konfiguration von **luci** mithilfe von **`/etc/sysconfig/luci`**“
- Abschnitt 2.5, „Konfiguration von ACPI zur Verwendung mit integrierten Fencing-Geräten“
- Abschnitt 2.6, „Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten“
- Abschnitt 2.7, „Überprüfung der Konfiguration“
- Abschnitt 2.8, „Überlegungen zum **`NetworkManager`**“
- Abschnitt 2.9, „Überlegungen zur Verwendung von Quorum Disk“
- Abschnitt 2.10, „Red Hat Hochverfügbarkeits-Add-On und SELinux“
- Abschnitt 2.11, „Multicast-Adressen“
- Abschnitt 2.12, „UDP-Unicast-Datenverkehr“
- Abschnitt 2.13, „Überlegungen zu **`ricci`**“
- Abschnitt 2.14, „Konfiguration von virtuellen Maschinen in einer Cluster-Umgebung“

2.1. Allgemeine Überlegungen zur Konfiguration

Sie können das Red Hat Hochverfügbarkeits-Add-On auf vielerlei Arten konfigurieren, um Ihren Bedürfnissen gerecht zu werden. Berücksichtigen Sie beim Planen, Konfigurieren und Implementieren Ihrer Bereitstellung die folgenden allgemeinen Überlegungen.

Anzahl der unterstützten Cluster-Knoten

Das Hochverfügbarkeits-Add-On unterstützt maximal 16 Cluster-Knoten.

Cluster an einem einzelnen Standort

Derzeit werden nur Cluster unterstützt, die sich an einem einzigen physischen Standort befinden. Cluster, die über mehrere physische Standorte verteilt sind, werden offiziell nicht unterstützt. Für weitere Einzelheiten und Informationen über Cluster an mehreren Standorten setzen Sie sich bitte mit Ihrem Red Hat Vertriebs- oder Kundendienstmitarbeiter in Verbindung.

GFS2

Obwohl das GFS2-Dateisystem sowohl auf einem eigenständigen System als auch als Teil einer Cluster-Konfiguration implementiert werden kann, unterstützt Red Hat den Einsatz von GFS2 nicht für ein Ein-Knoten-System. Red Hat unterstützt jedoch eine Reihe von leistungsstarken Ein-Knoten-Dateisystemen, die für den Einsatz auf einzelnen Knoten optimiert sind und dadurch meist einen geringeren Mehraufwand als ein Cluster-Dateisystem haben. Red Hat empfiehlt den Einsatz eines dieser Dateisysteme anstelle von GFS2 in Fällen, in denen nur

ein einzelner Knoten das Dateisystem einhängen muss. Red Hat wird für Bestandskunden weiterhin Ein-Knoten-GFS2-Dateisysteme unterstützen.

Wenn Sie ein GFS2-Dateisystem als ein Cluster-Dateisystem konfigurieren, müssen Sie sicherstellen, dass alle Knoten im Cluster Zugriff auf das gemeinsame Dateisystem haben. Asymmetrische Cluster-Konfigurationen, bei denen einige Knoten Zugriff auf den Speicher haben und andere nicht, werden nicht unterstützt. Es ist jedoch nicht nötig, dass alle Knoten das GFS2-Dateisystem auch tatsächlich selbst einhängen.

Hardware-Konfiguration ohne einzelne Ausfallpunkte

Cluster können ein Dual-Controller RAID-Array, mehrere gebündelte Netzwerkkanäle, mehrere Pfade zwischen Cluster-Mitgliedern und Speicher sowie UPS-Systeme ("Un-interruptible Power Supply" oder unterbrechungsfreie Stromversorgung) umfassen, um sicherzustellen, dass kein einzelner Ausfallpunkt zu Datenverlust oder Ausfallzeiten der Applikationen führt.

Alternativ kann ein kostengünstiger Cluster eingerichtet werden, der eine geringere Verfügbarkeit als ein Cluster ohne einzelnen Ausfallpunkt bietet. Beispielsweise können Sie einen Cluster mit einem Single-Controller RAID-Array und einem einzelnen Ethernet-Kanal einrichten.

Einige kostengünstige Alternativen, wie z.B. Host RAID Controller, Software RAID ohne Clustering-Unterstützung und parallele Multi-Initiator-SCSI-Konfigurationen sind nicht kompatibel bzw. nicht geeignet für den Einsatz als gemeinsam verwendeter Cluster-Speicher.

Gewährleistung der Datenintegrität

Um die Datenintegrität zu gewährleisten, darf zu jeder Zeit nur ein Knoten einen Cluster-Dienst ausführen und auf die zugehörigen Daten zugreifen. Mithilfe von Netzschaltern in der Cluster-Hardware-Konfiguration kann bei einem Ausfall ein Knoten einen anderen Knoten aus- und wieder einschalten, bevor dessen Hochverfügbarkeitsdienste neu gestartet werden. Dadurch wird verhindert, dass zwei Knoten gleichzeitig auf dieselben Daten zugreifen und diese dadurch beschädigen. Es wird dringend empfohlen, *Fencing-Geräte* (Hardware- oder Software-Lösungen, die extern Cluster-Knoten aus- und einschalten sowie neu starten können) einzusetzen, um selbst im Falle eines Ausfalls die Datenintegrität gewährleisten zu können.

Ethernet-Kanalbündelung

Das Cluster-Quorum und die Knoten-Zustände werden anhand von Meldungen bestimmt, die via Ethernet zwischen den Cluster-Knoten übertragen werden. Die Cluster-Knoten nutzen das Ethernet darüber hinaus für eine Vielzahl anderer kritischer Cluster-Features (z.B. das Fencing). Bei der Ethernet-Kanalbündelung werden mehrere Ethernet-Schnittstellen so konfiguriert, dass diese sich wie eine einzige Schnittstelle verhalten, wodurch das Risiko eines einzelnen Ausfallpunktes in der herkömmlichen Ethernet-Verbindung zwischen Cluster-Knoten und anderer Cluster-Hardware vermieden wird.

Von Red Hat Enterprise Linux 6.4 an werden die Bindungsarten 0, 1, and 2 unterstützt.

IPv4 und IPv6

Das Hochverfügbarkeits-Add-On unterstützt sowohl das IPv4- als auch das IPv6-Internetprotokoll. Die Unterstützung für IPv6 im Hochverfügbarkeits-Add-On ist neu für Red Hat Enterprise Linux 6.

2.2. Kompatible Hardware

Vergewissern Sie sich vor der Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software, dass Ihr Cluster geeignete Hardware verwendet (z.B. unterstützte Fencing-Geräte, Speichergeräte und Fibre

Channel Switches). Für die aktuellsten Informationen über kompatible Hardware werfen Sie einen Blick auf den Red Hat Hardware-Katalog unter https://hardware.redhat.com/.

2.3. Aktivieren von IP-Ports

Vor dem Einsatz des Red Hat Hochverfügbarkeits-Add-Ons müssen Sie bestimmte IP-Ports auf den Cluster-Knoten und auf Computern aktivieren, die **luci** (den Server für die **Conga** Benutzeroberfläche) ausführen. Die folgenden Abschnitte zeigen die IP-Ports, die aktiviert werden müssen:

- Abschnitt 2.3.1, „Aktivieren von IP-Ports auf Cluster-Knoten“
- Abschnitt 2.3.2, „Aktivieren des IP-Ports für **luci**“

Der folgende Abschnitt enthält die **`iptables`** Regeln für die Freigabe der IP-Ports, die von dem Red Hat Hochverfügbarkeits-Add-On benötigt werden:

- Abschnitt 2.3.3, „Konfiguration der iptables-Firewall zum Erlauben von Cluster-Komponenten“

2.3.1. Aktivieren von IP-Ports auf Cluster-Knoten

Damit die Knoten in einem Cluster miteinander kommunizieren können, müssen Sie die IP-Ports aktivieren, die bestimmten Red Hat Hochverfügbarkeits-Add-On-Komponenten zugewiesen sind. Tabelle 2.1, „Aktivierte IP-Ports auf Red Hat Hochverfügbarkeits-Add-On Knoten“ listet die IP-Port-Nummern auf, ihre entsprechenden Protokolle sowie die Komponenten, denen die Port-Nummern zugeordnet sind. Für jeden Cluster-Knoten aktivieren Sie die IP-Ports gemäß Tabelle 2.1, „Aktivierte IP-Ports auf Red Hat Hochverfügbarkeits-Add-On Knoten“. Sie können **`system-config-firewall`** verwenden, um die IP-Ports zu aktivieren.

Tabelle 2.1. Aktivierte IP-Ports auf Red Hat Hochverfügbarkeits-Add-On Knoten

IP-Port-Nummer	Protokoll	Komponente
5404, 5405	UDP	**`corosync/cman`** (Cluster-Manager)
11111	TCP	**`ricci`** (überträgt aktualisierte Cluster-Informationen)
21064	TCP	**`dlm`** (Distributed Lock Manager)
16851	TCP	**`modclusterd`**

2.3.2. Aktivieren des IP-Ports für luci

Um Client-Computern zu erlauben, mit einem Computer zu kommunizieren, der **luci** (den **Conga** Benutzeroberflächen-Server) ausführt, müssen Sie den IP-Port für **luci** aktivieren. Aktivieren Sie auf jedem Computer, der **luci** ausführt, die IP-Ports gemäß Tabelle 2.2, „Aktivierter IP-Port auf einem Computer, der luci ausführt“.



Anmerkung

Wenn ein Cluster-Knoten **luci** ausführt, sollte der Port 11111 bereits aktiviert sein.

Tabelle 2.2. Aktivierter IP-Port auf einem Computer, der luci ausführt

IP-Port-Nummer	Protokoll	Komponente
8084	TCP	**luci** (**Conga** Benutzeroberflächen-Server)

Ab der Red Hat Enterprise Linux 6.1 Release, in der die Konfiguration mithilfe der **`/etc/sysconfig/luci`** Datei vorgenommen wird, können Sie speziell festlegen, auf welcher IP-Adresse **luci** bereitgestellt werden soll. Diese Funktion kann nützlich sein, falls Ihre Serverinfrastruktur

mehr als ein Netzwerk umfasst und Sie nur vom internen Netzwerk auf **luci** zugreifen möchten. Entfernen Sie dazu die Kommentierung der Zeile, die den **host** spezifiziert. Um beispielsweise die **host** Einstellung in der Datei auf 10.10.10.10 zu ändern, bearbeiten Sie die **host** Zeile wie folgt:

```
host = 10.10.10.10
```

Für weitere Informationen über die **/etc/sysconfig/luci** Datei, siehe Abschnitt 2.4, „Konfiguration von **luci** mithilfe von **/etc/sysconfig/luci**“.

2.3.3. Konfiguration der iptables-Firewall zum Erlauben von Cluster-Komponenten

Nachstehend sehen Sie beispielhafte iptables-Regeln für die Aktivierung von IP-Ports, die von Red Hat Enterprise Linux 6 (mit Hochverfügbarkeits-Add-on) benötigt werden. Bitte beachten Sie, dass diese Beispiele 192.168.1.0/24 als Subnetz verwenden, aber Sie müssen 192.168.1.0/24 mit dem entsprechenden Subnetz ersetzen, wenn Sie diese Regeln verwenden.

Für **cman** (Cluster Manager) verwenden Sie die folgende Filterung.

```
$ iptables -I INPUT -m state --state NEW -m multiport -p udp -s 192.168.1.0/24
-d 192.168.1.0/24 --dports 5404,5405 -j ACCEPT
$ iptables -I INPUT -m addrtype --dst-type MULTICAST -m state --state NEW -m
multiport -p udp -s 192.168.1.0/24 --dports 5404,5405 -j ACCEPT
```

Für **dlm** (Distributed Lock Manager):

```
$ iptables -I INPUT -m state --state NEW -p tcp -s 192.168.1.0/24 -d
192.168.1.0/24 --dport 21064 -j ACCEPT
```

Für **ricci** (Teil des Conga Remote-Agent):

```
$ iptables -I INPUT -m state --state NEW -p tcp -s 192.168.1.0/24 -d
192.168.1.0/24 --dport 11111 -j ACCEPT
```

Für **modclusterd** (Teil des Conga Remote-Agent):

```
$ iptables -I INPUT -m state --state NEW -p tcp -s 192.168.1.0/24 -d
192.168.1.0/24 --dport 16851 -j ACCEPT
```

Für **luci** (Conga-Benutzeroberflächenserver):

```
$ iptables -I INPUT -m state --state NEW -p tcp -s 192.168.1.0/24 -d
192.168.1.0/24 --dport 8084 -j ACCEPT
```

Für **igmp** (Internet Group Management Protocol):

```
$ iptables -I INPUT -p igmp -j ACCEPT
```

Nach der Ausführung dieser Befehle führen Sie den folgenden Befehl aus, um die aktuelle Konfiguration dauerhaft zu speichern.

```
$ service iptables save ; service iptables restart
```

2.4. Konfiguration von luci mithilfe von /etc/sysconfig/luci

Ab der Red Hat Enterprise Linux 6.1 Release können Sie einige Verhaltensweisen von **luci** konfigurieren, indem Sie die **/etc/sysconfig/luci** Datei bearbeiten. Zu den Parametern, die Sie in dieser Datei ändern können, gehören Einstellungen zur laufenden Umgebung, die vom init-Skript

verwendet werden, sowie Einstellungen zur Serverkonfiguration. Zudem können Sie diese Datei bearbeiten, um einige Parameter zur Applikationskonfiguration anzupassen. In der Datei selbst finden Sie Anweisungen, welche Konfigurationsparameter Sie mithilfe dieser Datei ändern können.

Um das Format der Datei nicht zu beschädigen, sollten Sie keine der nicht konfigurierbaren Zeilen der **/etc/sysconfig/luci** Datei verändern, wenn Sie die Datei bearbeiten. Außerdem sollten Sie darauf achten, der erforderlichen Syntax für diese Datei zu folgen. Dies gilt insbesondere für den **INITSCRIPT** Abschnitt, der keinerlei Leerzeichen neben dem Gleichheitszeichen zulässt und Anführungszeichen um Zeichenketten erfordert, die Leerzeichen enthalten.

Das folgende Beispiel veranschaulicht, wie der Port, auf dem **luci** bereitgestellt wird, durch Bearbeiten der **/etc/sysconfig/luci** Datei verändert wird.

1. Entfernen Sie die Kommentierung der folgenden Zeile in der **/etc/sysconfig/luci** Datei:

   ```
   #port = 4443
   ```

2. Ersetzen Sie 4443 durch die gewünschte Port-Nummer, die größer oder gleich 1024 sein muss (kein privilegierter Port). Beispielsweise können Sie diese Zeile folgendermaßen bearbeiten, um den Port, auf dem **luci** bereitgestellt wird, auf 8084 festzulegen.

   ```
   port = 8084
   ```

3. Starten Sie den **luci** Dienst neu, damit die Änderungen wirksam werden.



Wichtig

Wenn Sie einen Konfigurationsparameter in der **/etc/sysconfig/luci** Datei anpassen, um einen Standardwert neu zu definieren, sollten Sie darauf achten, den neuen Wert anstelle des alten dokumentierten Werts zu verwenden. Wenn Sie beispielsweise den Port ändern möchten, auf dem **luci** bereitgestellt wird, achten Sie darauf, den neuen Wert anzugeben, wenn Sie einen IP-Port für **luci** aktivieren wie in Abschnitt 2.3.2, „Aktivieren des IP-Ports für **luci**“ beschrieben. Veränderte Port- und Host-Parameter werden automatisch in der URL widergespiegelt, wenn der **luci** Dienst startet, wie in Abschnitt 3.2, „Starten von **luci** “ beschrieben. Sie sollten diese URL verwenden, um auf **luci** zuzugreifen.

Eine vollständige Liste der Parameter, die Sie in der **/etc/sysconfig/luci** Datei konfigurieren können, finden Sie in der Dokumentation innerhalb der Datei selbst.

2.5. Konfiguration von ACPI zur Verwendung mit integrierten Fencing-Geräten

Falls Ihr Cluster integrierte Fencing-Geräte verwendet, müssen Sie ACPI ("Advanced Configuration and Power Interface") konfigurieren, um ein sofortiges und vollständiges Fencing (Datenabgrenzung) zu gewährleisten.



Anmerkung

Für die aktuellsten Informationen über integrierte Fencing-Geräte, die vom Red Hat Hochverfügbarkeits-Add-On unterstützt werden, siehe http://www.redhat.com/cluster_suite/hardware/.

Falls ein Cluster-Knoten zur Abgrenzung durch ein integriertes Fencing-Gerät konfiguriert ist, deaktivieren Sie ACPI Soft-Off für diesen Knoten. Das Deaktivieren des ACPI Soft-Off erlaubt es einem

integrierten Fencing-Gerät, einen Knoten sofort und vollständig abzuschalten, statt diesen sauber herunterzufahren (z.B. **`shutdown -h now`**). Bleibt ACPI Soft-Off dagegen aktiviert, braucht ein integriertes Fencing-Gerät vier Sekunden oder länger, um einen Knoten abzuschalten (siehe nachfolgende Anmerkung). Zudem ist mit aktiviertem ACPI Soft-Off ein integriertes Fencing-Gerät unter Umständen nicht dazu in der Lage, einen Knoten abzuschalten, der während des Herunterfahrens hängenbleibt. Unter diesen Umständen würde die Abgrenzung erst verzögert erfolgen oder ganz fehlschlagen. Wenn ein Knoten mit einem integrierten Fencing-Gerät abgegrenzt wird und ACPI Soft-Off aktiviert ist, würde sich ein Cluster infolgedessen nur sehr langsam erholen oder gar administratives Eingreifen erfordern.



Anmerkung

Die Zeit, die zum Abgrenzen eines Knotens benötigt wird, hängt von dem verwendeten integrierten Fencing-Gerät ab. Die Leistung einiger integrierter Fencing-Geräte ist vergleichbar mit dem gedrückt Halten des Ein-/Ausschaltknopfes; das Fencing-Gerät benötigt demnach etwa vier bis fünf Sekunden zum Ausschalten des Knotens. Die Leistung anderer integrierter Fencing-Geräte ist vergleichbar mit einem kurzen Drücken des Ein-/Ausschaltknopfes; das Fencing-Gerät verlässt sich also auf das Betriebssystem zum Ausschalten des Knotens und benötigt demnach eine sehr viel längere Zeit als vier oder fünf Sekunden zum Ausschalten des Knotens.

Um ACPI Soft-Off zu deaktivieren, verwenden Sie den **`chkconfig`** Befehl und überprüfen Sie, dass der Knoten bei einer Abgrenzung tatsächlich sofort abgeschaltet wird. Die bevorzugte Methode zum Deaktivieren von ACPI Soft-Off ist der **`chkconfig`** Befehl. Falls diese Methode in Ihrem Cluster nicht das gewünschte Ergebnis erzielt, können Sie ACPI Soft-Off auch mit einer der folgenden, alternativen Methoden deaktivieren:

- Ändern Sie die BIOS-Einstellung auf "instant-off" oder auf eine ähnliche Einstellung, die den Knoten ohne Verzögerung abschaltet.

  Anmerkung

  Das Deaktivieren von ACPI Soft-Off im BIOS steht auf einigen Computern ggf. nicht zur Verfügung.

- Fügen Sie **`acpi=off`** zu der Kernel-Boot-Befehlszeile der **`/boot/grub/grub.conf`** Datei hinzu.

  Wichtig

  Diese Methode deaktiviert ACPI vollständig; einige Computer fahren jedoch ggf. nicht einwandfrei hoch, wenn ACPI vollständig deaktiviert ist. Nutzen Sie diese Methode *nur dann*, wenn die anderen gezeigten Methoden für Ihren Cluster nicht zum gewünschten Ergebnis führen.

Die folgenden Abschnitte zeigen die Verfahren der bevorzugten Methode sowie der alternativen Methoden zum Deaktivieren von ACPI Soft-Off:

- Abschnitt 2.5.1, „Deaktivieren von ACPI Soft-Off mit dem **`chkconfig`** Befehl“ — Bevorzugte Methode
- Abschnitt 2.5.2, „Deaktivieren von ACPI Soft-Off im BIOS“ — Erste alternative Methode
- Abschnitt 2.5.3, „Vollständiges Deaktivieren von ACPI in der **`grub.conf`** Datei“ — Zweite alternative Methode

2.5.1. Deaktivieren von ACPI Soft-Off mit dem `chkconfig` Befehl

Sie können den **`chkconfig`** Befehl zur Deaktivierung von ACPI Soft-Off verwenden, indem Sie entweder

den ACPI-Daemon (**acpid**) aus der **chkconfig** Verwaltung entfernen, oder indem Sie **acpid** ausschalten.



Anmerkung

Dies ist die bevorzugte Methode zur Deaktivierung von ACPI Soft-Off.

Deaktivieren Sie ACPI Soft-Off auf jedem Cluster-Knoten mit dem **chkconfig** Befehl, und zwar wie folgt:

1. Führen Sie einen dieser beiden Befehle aus:
   - **chkconfig --del acpid** — Dieser Befehl entfernt **acpid** aus der **chkconfig** Verwaltung.

     — ODER —
   - **chkconfig --level 345 acpid off** — Dieser Befehl schaltet **acpid** aus.
2. Starten Sie den Knoten neu.
3. Wenn der Cluster konfiguriert ist und läuft, vergewissern Sie sich, dass der Knoten bei einer Abgrenzung sofort abgeschaltet wird.

   Anmerkung

   Sie können den Knoten mittels dem **fence_node** Befehl oder mit **Conga** abgrenzen.

2.5.2. Deaktivieren von ACPI Soft-Off im BIOS

Die bevorzugte Methode zum Deaktivieren von ACPI Soft-Off ist mittels **chkconfig** Befehl (Abschnitt 2.5.1, „Deaktivieren von ACPI Soft-Off mit dem **chkconfig** Befehl“). Führt die bevorzugte Methode jedoch nicht zum gewünschten Ergebnis, folgen Sie den in diesem Abschnitt beschriebenen Verfahren.



Anmerkung

Das Deaktivieren von ACPI Soft-Off im BIOS steht auf einigen Computern ggf. nicht zur Verfügung.

Sie können ACPI Soft-Off deaktivieren, indem Sie das BIOS in jedem Cluster-Knoten wie folgt konfigurieren:

1. Starten Sie den Knoten neu und starten Sie das **BIOS CMOS Setup Utility** Programm.
2. Navigieren Sie zum **Power** Menü (oder ähnliches Menü zur Energieverwaltung).
3. Setzen Sie im **Power** Menü die **Soft-Off by PWR-BTTN** Funktion (oder ähnlich) auf **Instant-Off** (oder eine ähnliche Einstellung, die den Knoten über den Ein-/Ausschaltknopf ohne Verzögerung ausschaltet). Beispiel 2.1, „**BIOS CMOS Setup Utility**: Soft-Off by PWR-BTTN auf Instant-Off eingestellt“ zeigt ein **Power** Menü mit der **ACPI Function** auf **Enabled** (aktiviert) und **Soft-Off by PWR-BTTN** auf **Instant-Off** (sofort ausschalten) eingestellt.

   Anmerkung

   Abhängig von Ihrem Computertyp heißen die Menüpunkte **ACPI Function**, **Soft-Off by PWR-BTTN** und **Instant-Off** ggf. anders. Das Ziel dieses Verfahren ist es jedoch, das BIOS dahingehend zu konfigurieren, dass der Computer durch Betätigen des Ein-/Ausschaltknopfes ohne Verzögerung abgeschaltet wird.

4. Verlassen Sie das **`BIOS CMOS Setup Utility`** Programm und speichern so die BIOS-Konfiguration.
5. Wenn der Cluster konfiguriert ist und läuft, vergewissern Sie sich, dass der Knoten bei einer Abgrenzung sofort abgeschaltet wird.



Anmerkung

Sie können den Knoten mittels dem **`fence_node`** Befehl oder mit **Conga** abgrenzen.

Beispiel 2.1. `BIOS CMOS Setup Utility`: Soft-Off by PWR-BTTN auf Instant-Off eingestellt

```
+---------------------------------------------|-------------------+
|    ACPI Function             [Enabled]      |    Item Help      |
|    ACPI Suspend Type         [S1(POS)]      |-------------------|
|  x Run VGABIOS if S3 Resume   Auto          |   Menu Level   *  |
|    Suspend Mode              [Disabled]     |                   |
|    HDD Power Down            [Disabled]     |                   |
|    Soft-Off by PWR-BTTN      [Instant-Off   |                   |
|    CPU THRM-Throttling       [50.0%]        |                   |
|    Wake-Up by PCI card       [Enabled]      |                   |
|    Power On by Ring          [Enabled]      |                   |
|    Wake Up On LAN            [Enabled]      |                   |
|  x USB KB Wake-Up From S3     Disabled      |                   |
|    Resume by Alarm           [Disabled]     |                   |
|  x  Date(of Month) Alarm       0            |                   |
|  x  Time(hh:mm:ss) Alarm       0 :  0 :     |                   |
|    POWER ON Function         [BUTTON ONLY   |                   |
|  x KB Power ON Password       Enter         |                   |
|  x Hot Key Power ON           Ctrl-F1       |                   |
|                                             |                   |
|                                             |                   |
+---------------------------------------------|-------------------+
```

Dieses Beispiel zeigt die **ACPI Function** auf **Enabled** (aktiviert) und **Soft-Off by PWR-BTTN** auf **Instant-Off** (sofort ausschalten) eingestellt.

2.5.3. Vollständiges Deaktivieren von ACPI in der `grub.conf` Datei

Die bevorzugte Methode zum Deaktivieren von ACPI Soft-Off ist mittels **`chkconfig`** Befehl (Abschnitt 2.5.1, „Deaktivieren von ACPI Soft-Off mit dem **`chkconfig`** Befehl“). Führt die bevorzugte Methode jedoch nicht zum gewünschten Ergebnis, können Sie ACPI Soft-Off in der Energieverwaltung des BIOS deaktivieren (Abschnitt 2.5.2, „Deaktivieren von ACPI Soft-Off im BIOS“). Falls in Ihrem Cluster keine dieser beiden Methoden zum Ziel führt, können Sie ACPI vollständig deaktiveren, indem Sie **`acpi=off`** an die Kernel-Boot-Befehlszeile der **`grub.conf`** Datei anhängen.



Wichtig

Diese Methode deaktiviert ACPI vollständig; einige Computer fahren jedoch ggf. nicht einwandfrei hoch, wenn ACPI vollständig deaktiviert ist. Nutzen Sie diese Methode *nur dann*, wenn die anderen gezeigten Methoden für Ihren Cluster nicht zum gewünschten Ergebnis führen.

Sie können ACPI vollständig deaktivieren, indem Sie die **`grub.conf`** Datei in jedem Cluster-Knoten wie folgt bearbeiten:

1. Öffnen Sie **/boot/grub/grub.conf** mit einem Texteditor.
2. Fügen Sie **acpi=off** am Ende der Kernel-Boot-Befehlszeile in **/boot/grub/grub.conf** hinzu (siehe Beispiel 2.2, „Kernel-Boot-Befehlszeile mit angefügtem **acpi=off**“).
3. Starten Sie den Knoten neu.
4. Wenn der Cluster konfiguriert ist und läuft, vergewissern Sie sich, dass der Knoten bei einer Abgrenzung sofort abgeschaltet wird.



Anmerkung

Sie können den Knoten mittels dem **fence_node** Befehl oder mit **Conga** abgrenzen.

Beispiel 2.2. Kernel-Boot-Befehlszeile mit angefügtem acpi=off

```
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/mapper/vg_doc01-lv_root
#          initrd /initrd-[generic-]version.img
#boot=/dev/hda
default=0
timeout=5
serial --unit=0 --speed=115200
terminal --timeout=5 serial console
title Red Hat Enterprise Linux Server (2.6.32-193.el6.x86_64)
        root (hd0,0)
        kernel /vmlinuz-2.6.32-193.el6.x86_64 ro root=/dev/mapper/vg_doc01-
lv_root console=ttyS0,115200n8 acpi=off
        initrd /initramrs-2.6.32-131.0.15.el6.x86_64.img
```

In diesem Beispiel wurde **acpi=off** am Ende der Kernel-Boot-Befehlszeile — die Zeile, die mit "kernel /vmlinuz-2.6.32-193.el6.x86_64.img" beginnt — angefügt.

2.6. Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten

Sie können Ihren Cluster auf Ihre Anforderungen zur Hochverfügbarkeit anpassen, indem Sie Hochverfügbarkeitsdienste konfigurieren. Die Schlüsselkomponente zur Verwaltung von Hochverfügbarkeitsdiensten im Red Hat Hochverfügbarkeits-Add-On, **rgmanager**, implementiert Ausfallsicherung für Standardapplikationen. Im Red Hat Hochverfügbarkeits-Add-On wird eine Applikation mit anderen Cluster-Ressourcen konfiguriert, um einen Hochverfügbarkeitsdienst zu bilden, der zur Ausfallsicherung von einem Cluster-Knoten auf einen anderen wechseln kann, ohne signifikante Unterbrechung für Cluster-Clients. Das Wechseln eines Hochverfügbarkeitsdienstes auf einen anderen Knoten kann z.B. erfolgen, wenn ein Cluster-Knoten ausfällt oder ein Cluster-Systemadministrator den Dienst von einem Cluster-Knoten auf einen anderen verlegt (z.B. für eine geplante Betriebsunterbrechung eines Cluster-Knotens).

Um einen Hochverfügbarkeitsdienst zu erstellen, müssen Sie diesen in der Cluster-Konfigurationsdatei konfigurieren. Ein Hochverfügbarkeitsdienst besteht aus Cluster-*Ressourcen*. Cluster-Ressourcen bilden Blöcke, die Sie in der Cluster-Konfigurationsdatei erstellen und verwalten können — beispielsweise eine IP-Adresse, ein Skript zur Initialisierung einer Applikation oder eine gemeinsam genutzte Red Hat GFS2-Partition.

Ein Hochverfügbarkeitsdienst darf zur Gewährleistung der Datenintegrität zu jeder Zeit nur auf einem einzigen Cluster-Knoten laufen. Sie können eine Ausfallsicherungspriorität in einer Ausfallsicherungs-Domain angeben. Die Angabe einer solchen Ausfallsicherungspriorität besteht aus der Zuweisung eines Prioritätslevels für jeden Knoten in einer Ausfallsicherungs-Domain. Das Prioritätslevel bestimmt die Reihenfolge der Ausfallsicherung — dabei wird ermittelt, auf welchen Knoten ein Hochverfügbarkeitsdienst im Falle eines Ausfalls wechseln soll. Falls Sie keine Ausfallsicherungspriorität angeben, kann ein Hochverfügbarkeitsdienst im Falle eines Ausfalls auf jeden beliebigen Knoten innerhalb seiner Ausfallsicherungs-Domain wechseln. Auch können Sie angeben, ob ein Hochverfügbarkeitsdienst so eingeschränkt werden soll, dass er nur auf Knoten seiner zugewiesenen Ausfallsicherungs-Domains läuft. (Ist ein Hochverfügbarkeitsdienst mit einer uneingeschränkten Ausfallsicherungs-Domain verknüpft, kann er für den Fall, dass kein Mitglied der Ausfallsicherungs-Domain zur Verfügung steht, auf jedem beliebigen Cluster-Knoten starten.)

Abbildung 2.1, „Beispiel: Webserver-Cluster-Dienst “ zeigt ein Beispiel eines Hochverfügbarkeitsdienstes, nämlich einen Webserver mit der Bezeichnung "content-webserver". Er läuft auf Cluster-Knoten B und befindet sich in einer Ausfallsicherungs-Domain, die aus den Knoten A, B und D besteht. Zusätzlich ist die Ausfallsicherungs-Domain mit einer Ausfallsicherungspriorität konfiguriert, um im Falle eines Ausfalls auf den Knoten D zu wechseln, bevor auf Knoten A gewechselt wird und um die Ausfallsicherung nur auf Knoten aus dieser Ausfallsicherungs-Domain zu beschränken. Der Hochverfügbarkeitsdienst umfasst die folgenden Cluster-Ressourcen:

- IP-Adressen-Ressource — IP-Adresse 10.10.10.201.
- Eine Applikations-Ressource mit dem Namen "httpd-content" — Ein Initialisierungsskript **`/etc/init.d/httpd`** für eine Webserver-Applikation (nämlich **`httpd`**).
- Eine Dateisystem-Ressource — Red Hat GFS2, genannt "gfs2-content-webserver".

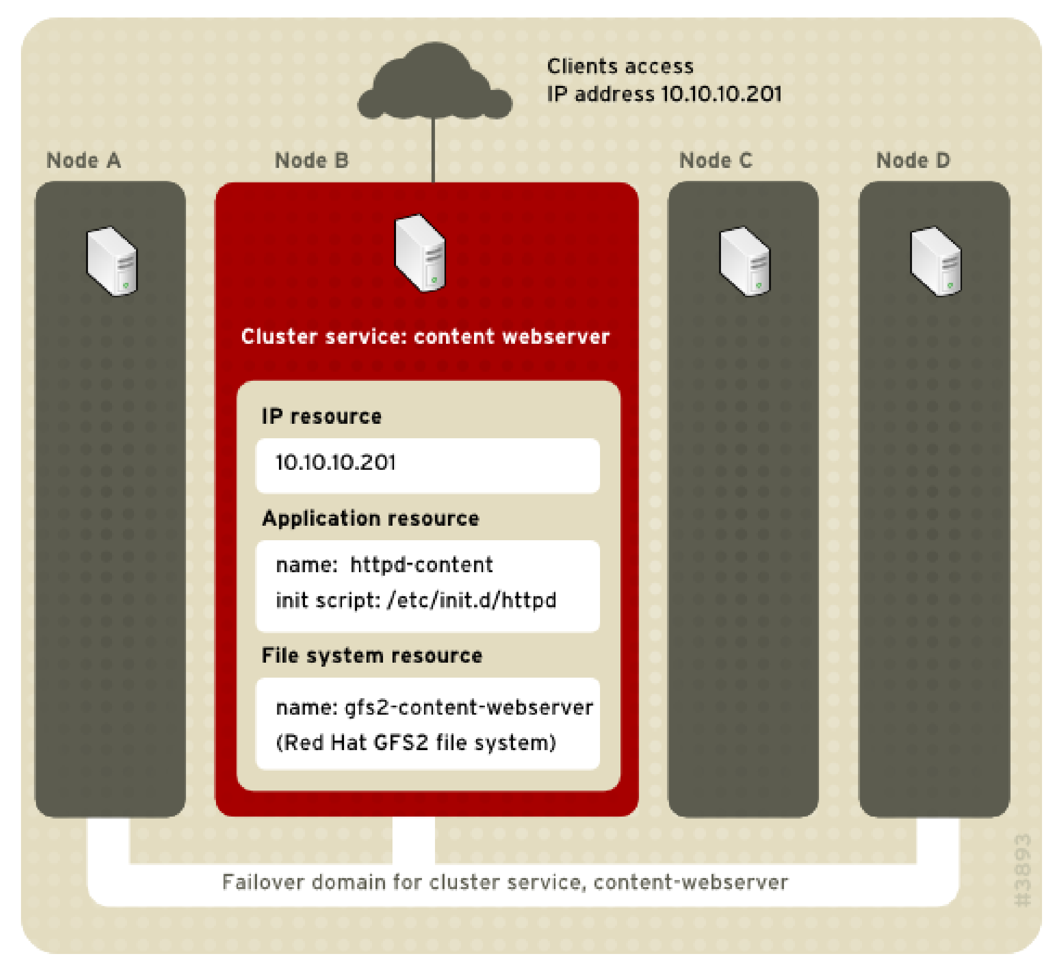


Abbildung 2.1. Beispiel: Webserver-Cluster-Dienst

Clients greifen auf den Cluster-Dienst via IP-Adresse 10.10.10.201 zu, was eine Interaktion mit der Webserver-Applikation, httpd-content, ermöglicht. Die Applikation "httpd-content" verwendet das "gfs2-content-webserver"-Dateisystem. Falls der Knoten B ausfallen sollte, würde der Hochverfügbarkeitsdienst "content-webserver" auf Knoten D wechseln. Falls Knoten D nicht verfügbar sein sollte oder auch ausgefallen ist, würde der Dienst auf Knoten A wechseln. Die Ausfallsicherung würde ohne nennenswerte Unterbrechung für Cluster-Clients erfolgen. In einem HTTP-Dienst beispielsweise könnten hierdurch lediglich gewisse Zustandsinformationen verloren gehen (z.B. Sitzungsdaten). Der Hochverfügbarkeitsdienst wäre von einem anderen Cluster-Knoten aus unter derselben IP-Adresse erreichbar wie vor der Ausfallsicherung.



Anmerkung

Weitere Informationen über Hochverfügbarkeitsdienste und Ausfallsicherungs-Domains finden Sie im Handbuch *Überblick über das Hochverfügbarkeits-Add-On*. Informationen über die Konfiguration von Ausfallsicherungs-Domains finden Sie in Kapitel 3, *Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit **Conga*** (unter Verwendung von **Conga**) oder Kapitel 7, *Manuelle Konfiguration von Red Hat Hochverfügbarkeit* (unter Verwendung der Befehlszeilen-Tools).

Ein Hochverfügbarkeitsdienst besteht aus einer Gruppe von Cluster-Ressourcen, die als eine zusammenhängende Einheit konfiguriert wurden und zusammen einen spezialisierten Dienst für Clients bereitstellen. Ein Hochverfügbarkeitsdienst wird als Ressourcenbaum in der Cluster-Konfigurationsdatei **`/etc/cluster/cluster.conf`** dargestellt (in jedem Cluster-Knoten). In der Cluster-Konfigurationsdatei ist jeder Ressourcenbaum eine XML-Darstellung, die jede Ressource spezifiziert, deren Parameter, sowie ihre Relationen zu anderen Ressourcen im Ressourcenbaum (Eltern-, Kind-, Geschwisterrelationen).



Anmerkung

Da ein Hochverfügbarkeitsdienst aus Ressourcen besteht, die in einem hierarchischen Baum angeordnet sind, wird ein solcher Dienst manchmal auch als *Ressourcenbaum* oder *Ressourcengruppe* bezeichnet. Beide Ausdrücke sind Synonyme für *Hochverfügbarkeitsdienst*.

An der Wurzel eines jeden Ressourcenbaums befindet sich eine besondere Art von Ressource — eine *Dienstressource*. Andere Arten von Ressourcen bilden den Rest eines Dienstes und bestimmen so dessen Charakteristiken. Zum Erstellen eines Hochverfügbarkeitsdienstes gehört das Erstellen einer Dienstressource, das Erstellen untergeordneter Cluster-Ressourcen, sowie deren Anordnung in eine zusammenhängende Einheit gemäß den hierarchischen Einschränkungen des Dienstes.

Zwei grundlegende Überlegungen sollten bei der Konfiguration eines Hochverfügbarkeitsdienstes berücksichtigt werden:

- Die Ressourcenarten, die zum Erstellen eines Dienstes nötig sind
- Eltern-, Kind- und Geschwisterrelationen zwischen den Ressourcen

Die Arten der Ressourcen und deren Hierarchie hängen von der Art des Dienstes ab, den Sie konfigurieren.

Die Arten von Cluster-Ressourcen sind in Anhang B, *Parameter der Hochverfügbarkeitsressourcen* aufgelistet. Informationen über Eltern-, Kind- und Geschwisterrelationen unter den Ressourcen finden Sie in Anhang C, *Verhalten der Hochverfügbarkeitsressourcen*.

2.7. Überprüfung der Konfiguration

Die Cluster-Konfiguration wird während des Starts und beim Neuladen einer Konfiguration automatisch

anhand des Cluster-Schemas unter **/usr/share/cluster/cluster.rng** überprüft. Zudem können Sie eine Cluster-Konfiguration jederzeit mithilfe des **ccs_config_validate** Befehls überprüfen. Informationen über die Konfigurationsprüfung bei der Verwendung des **ccs** Befehls finden Sie unter Abschnitt 5.1.6, „Überprüfung der Konfiguration“.

Ein kommentiertes Schema steht unter **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** zur Ansicht (z.B. **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

Bei der Konfigurationsprüfung wird auf folgende Fehler hin überprüft:

- XML-Gültigkeit — Überprüft, ob die Konfigurationsdatei eine gültige XML-Datei ist.
- Konfigurationsoptionen — Überprüft, ob Optionen (XML-Elemente und Parameter) gültig sind.
- Optionswerte — Überprüft, ob die Optionen gültige Daten enthalten (begrenzt).

Die folgenden Beispiele zeigen eine gültige Konfiguration und mehrere ungültige Konfigurationen, um die Gültigkeitsüberprüfungen zu veranschaulichen:

- Gültige Konfiguration — Beispiel 2.3, „**cluster.conf** Beispielkonfiguration: Gültige Datei“
- Ungültiges XML — Beispiel 2.4, „**cluster.conf** Beispielkonfiguration: Ungültiges XML“
- Ungültige Option — Beispiel 2.5, „**cluster.conf** Beispielkonfiguration: Ungültige Option“
- Ungültiger Optionswert — Beispiel 2.6, „**cluster.conf** Beispielkonfiguration: Ungültiger Optionswert“

Beispiel 2.3. cluster.conf Beispielkonfiguration: Gültige Datei

```
<cluster name="mycluster" config_version="1">
  <logging debug="off"/>
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Beispiel 2.4. `cluster.conf` Beispielkonfiguration: Ungültiges XML

```
<cluster name="mycluster" config_version="1">
  <logging debug="off"/>
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
<cluster>         <----------------INVALID
```

In diesem Beispiel fehlt in der letzten Zeile der Konfiguration (hier kommentiert als "INVALID", also ungültig) ein Schrägstrich — es steht hier **`<cluster>`** anstelle von **`</cluster>`**.

Beispiel 2.5. `cluster.conf` Beispielkonfiguration: Ungültige Option

```
<cluster name="mycluster" config_version="1">
  <loging debug="off"/>         <----------------INVALID
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
<cluster>
```

In diesem Beispiel enthält die zweite Zeile der Konfiguration (hier kommentiert als "INVALID", also ungültig) ein ungültiges XML-Element — es steht hier **`loging`** anstelle von **`logging`**.

Beispiel 2.6. `cluster.conf` Beispielkonfiguration: Ungültiger Optionswert

```
<cluster name="mycluster" config_version="1">
  <loging debug="off"/>
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="-1">  <--------INVALID
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
<cluster>
```

In diesem Beispiel enthält die vierte Zeile der Konfiguration (hier kommentiert als "INVALID", also ungültig) einen ungültigen Wert für den XML-Parameter, **`nodeid`** in der **`clusternode`** Zeile für **`node-01.example.com`**. Der Wert hier ist ein negativer Wert ("-1") anstelle eines positiven Werts ("1"). Für den **`nodeid`** Parameter muss der Wert jedoch positiv sein.

2.8. Überlegungen zum NetworkManager

Die Verwendung des **`NetworkManagers`** wird auf Cluster-Knoten nicht unterstützt. Wenn Sie den **`NetworkManager`** auf Ihren Cluster-Knoten installiert haben, sollten Sie diesen entweder entfernen oder deaktivieren.



Anmerkung

Der **`cman`** Dienst wird nicht starten, wenn der **`NetworkManager`** läuft oder mithilfe des **`chkconfig`** Befehls zur Ausführung konfiguriert wurde.

2.9. Überlegungen zur Verwendung von Quorum Disk

Quorum Disk ist ein datenträgerbasierter Quorum-Daemon, **`qdiskd`**, der ergänzende Heuristiken zum Bestimmen der Knotengesundheit liefert. Mit Heuristiken können Sie Faktoren bestimmen, die wichtig für die Funktion des Knotens im Falle einer Spaltung des Clusters sind. In einem Cluster mit vier Knoten und einer 3:1-Spaltung beispielsweise "gewinnen" die drei Knoten für gewöhnlich automatisch aufgrund Ihrer 3-zu-1-Mehrheit. In dieser Situation wird der einzelne Knoten abgegrenzt. Mithilfe von **`qdiskd`** können Sie dagegen Heuristiken einrichten, die es dem einzelnen Knoten ermöglichen zu gewinnen, basierend auf dessen Zugriff auf eine kritische Ressource (z.B. ein kritischer Netzwerkpfad). Falls Ihr Cluster zusätzliche Methoden zur Bestimmung der Knotengesundheit erfordert, sollten Sie zu diesem Zweck **`qdiskd`** konfigurieren.



Anmerkung

Das Konfigurieren von **qdiskd** ist nur dann notwendig, wenn Sie besondere Anforderungen an die Knotengesundheit haben. Beispiel für eine besondere Anforderung wäre eine "all-but-one" (alle-außer-einem) Konfiguration. In einer "all-but-one"-Konfiguration wird **qdiskd** so konfiguriert, dass genügend Quorum-Stimmen geliefert werden, um das Quorum zu erhalten, selbst wenn nur ein einziger Knoten läuft.



Wichtig

Heuristiken und andere **qdiskd** Parameter für Ihre Bereitstellung hängen im Wesentlichen von den Anforderungen Ihrer Umgebung und sonstigen besonderen Anforderungen ab. Für das bessere Verständnis der Verwendung von Heuristiken und anderen **qdiskd** Parametern werfen Sie einen Blick auf die qdisk(5) Handbuchseite. Falls Sie beim Einsatz von **qdiskd** in Ihrer Umgebung Hilfe benötigen, setzen Sie sich bitte mit einem autorisierten Red Hat Support-Vertreter in Verbindung.

Wenn Sie **qdiskd** einsetzen müssen, sollten Sie folgende Faktoren berücksichtigen:

Cluster-Knotenstimmen

Wird Quorum Disk verwendet, muss jeder Cluster-Knoten eine Stimme haben.

Timeout für CMAN-Mitgliedschaft

Der Wert für den **qdiskd**-Mitgliedschafts-Timeout wird automatisch konfiguriert basierend auf dem Wert für den CMAN-Mitgliedschafts-Timeout (die Zeit, die ein Knoten nicht reagiert, bevor CMAN - kurz für Cluster-Manager - diesen Knoten als tot betrachtet, und nicht mehr als Mitglied). **qdiskd** führt zudem zusätzliche Überprüfungen durch, um sicherzustellen, dass er innerhalb der Zeit für den CMAN-Timeout operieren kann. Falls Sie diesen Wert anpassen müssen, sollten Sie Folgendes beachten:

Der Wert für den CMAN-Mitgliedschafts-Timeout sollte mindestens doppelt so lang sein, wie der Wert für den **qdiskd**-Mitgliedschafts-Timeout. Der Grund hierfür ist der, dass der Quorum-Daemon ausgefallene Knoten selbst entdecken muss und hierzu ggf. deutlich länger braucht als der CMAN. Andere umgebungsspezifische Bedingungen können das Verhältnis zwischen den Mitgliedschafts-Timeout-Werten von CMAN und **qdiskd** beeinflussen. Falls Sie beim Anpassen des Werts für den CMAN-Mitgliedschafts-Timeout Hilfe benötigen, setzen Sie sich bitte mit einem autorisierten Red Hat Support-Vertreter in Verbindung.

Fencing (Datenabgrenzung)

Um beim Einsatz von **qdiskd** zuverlässiges Fencing zu gewährleisten, verwenden Sie Power-Fencing. Für Cluster ohne **qdiskd** können zwar auch andere Arten von Fencing zuverlässig arbeiten, diese sind jedoch für einen Cluster, der mit **qdiskd** konfiguriert ist, nicht ausreichend zuverlässig.

Höchstanzahl von Knoten

Ein Cluster, der mit **qdiskd** konfiguriert ist, unterstützt maximal 16 Knoten. Der Grund für diese Grenze liegt in der Skalierbarkeit; eine Erhöhung der Knotenanzahl geht mit einer Erhöhung der synchronen I/O-Auslastung auf dem gemeinsam verwendeten Quorumdatenträger einher.

Quorumdatenträger

Ein Quorumdatenträger sollte ein gemeinsam verwendetes Blockgerät sein mit parallelem Lese-

/Schreibzugriff für alle Knoten in einem Cluster. Die Mindestgröße für das Blockgerät sollte 10 Megabytes betragen. Zu den gemeinsam verwendeten Blockgeräten, die von **qdiskd** verwendet werden können, gehören z.B. ein Multi-Port SCSI RAID Array, ein Fibre Channel RAID SAN oder ein RAID-konfiguriertes iSCSI-Ziel. Sie können einen Quorumdatenträger mit dem Dienstprogramm für Cluster-Quorumdatenträger **mkqdisk** erstellen. Weitere Informationen über die Verwendung dieses Dienstprogramms finden Sie auf der mkqdisk(8) Handbuchseite.



Anmerkung

Der Einsatz von JBOD als Quorumdatenträger wird nicht empfohlen. Eine JBOD bietet keine zuverlässige Leistung und könnte daher einem Knoten einen Schreibvorgang nicht schnell genug ermöglichen. Kann ein Knoten nicht schnell genug auf einen Quorumdatenträger schreiben, wird dieser Knoten fälschlicherweise aus dem Cluster ausgeschlossen.

2.10. Red Hat Hochverfügbarkeits-Add-On und SELinux

Das Hochverfügbarkeits-Add-On für Red Hat Enterprise Linux 6 unterstützt SELinux im **enforcing** Modus mit der SELinux-Richtlinie auf **targeted** eingestellt.



Anmerkung

Wenn Sie SELinux zusammen mit dem Hochverfügbarkeits-Add-On in einer VM-Umgebung einsetzen, sollten Sie sicherstellen, dass die boolsche SELinux-Variable SELinux **fenced_can_network_connect** dauerhaft auf **on** gesetzt ist. Dies ermöglicht dem **fence_xvm** Fencing-Agent die ordnungsgemäße Ausführung, so dass das System virtuelle Maschinen abgrenzen kann.

Weitere Informationen über SELinux finden Sie im *Bereitstellungshandbuch* für Red Hat Enterprise Linux 6.

2.11. Multicast-Adressen

Die Knoten in einem Cluster kommunizieren untereinander mit Multicast-Adressen. Daher muss jeder Netzwerk-Switch und zugehörige Netzwerkkomponenten im Red Hat Hochverfügbarkeits-Add-On dazu konfiguriert sein, Multicast-Adressen zu ermöglichen und IGMP (Internet Group Management Protocol) zu unterstützen. Stellen Sie sicher, dass jeder Netzwerk-Switch und die zugehörigen Netzwerkkomponenten im Red Hat Hochverfügbarkeits-Add-On dazu in der Lage sind, IGMP und Multicast-Adressen zu unterstützen; wenn sie es können, stellen Sie sicher, dass Multicast-Adressierung und IGMP aktiviert sind. Ohne Multicast und IGMP können sich nicht alle Knoten in einem Cluster beteiligen, wodurch der Cluster scheitert. Verwenden Sie in solchen Umgebungen UDP Unicast, wie in Abschnitt 2.12, „UDP-Unicast-Datenverkehr“ beschrieben.



Anmerkung

Verfahren zur Konfiguration von Netzwerk-Switches und zugehörigen Netzwerkgeräten unterscheiden sich je nach Produkt. Lesen Sie bitte die entsprechende Herstellerdokumentation oder andere Informationsquellen für Informationen darüber, wie für diese Netzwerk-Switches und Netzwerkgeräte Multicast-Adressen und IGMP aktiviert werden können.

2.12. UDP-Unicast-Datenverkehr

Ab der Red Hat Enterprise Linux 6.2 Release können die Knoten in einem Cluster miteinander über den UDP-Unicast-Transportmechanismus kommunizieren. Es wird jedoch empfohlen, dass Sie IP-Multicasting für das Cluster-Netzwerk verwenden. UDP-Unicast ist eine Alternative, die verwendet werden kann, wenn IP-Multicasting nicht zur Verfügung steht.

Sie können das Red Hat Hochverfügbarkeits-Add-On zur Konfiguration von UDP-Unicast konfigurieren, indem Sie den **cman transport="udpu"** Parameter in der **cluster.conf** Konfigurationsdatei erstellen. Sie können Unicast auch auf der **Netzwerkkonfiguration** Seite der **Conga** Benutzeroberfläche, wie in Abschnitt 3.5.3, „Konfiguration des Netzwerks“ beschrieben, konfigurieren.

2.13. Überlegungen zu ricci

In Red Hat Enterprise Linux 6 löst **ricci** nunmehr **ccsd** ab. Es ist deshalb notwendig, dass **ricci** auf jedem Cluster-Knoten ausgeführt wird, um entweder mithilfe des **cman_tool version -r** Befehls, des **ccs** Befehls oder mithilfe des **luci** Benutzeroberflächen-Servers aktualisierte Cluster-Konfigurationsinformationen im Cluster verbreiten zu können. Sie können **ricci** starten, indem Sie **service ricci start** ausführen oder indem Sie mithilfe von **chkconfig** festlegen, dass es beim Systemstart automatisch starten soll. Informationen über das Aktivieren von IP-Ports für **ricci** finden Sie in Abschnitt 2.3.1, „Aktivieren von IP-Ports auf Cluster-Knoten“.

Ab der Red Hat Enterprise Linux 6.1 Release erfordert **ricci** ein Passwort, wenn Sie zum ersten Mal aktualisierte Cluster-Konfigurationen von einem bestimmten Knoten verbreiten möchten. Sie richten das **ricci** Passwort nach der Installation von **ricci** auf Ihrem System ein, indem Sie als Root den Befehl **passwd ricci** für den Benutzer **ricci** ausführen.

2.14. Konfiguration von virtuellen Maschinen in einer Cluster-Umgebung

Wenn Sie Ihren Cluster mit virtuellen Maschinen-Ressourcen konfigurieren, sollten Sie die **rgmanager** Tools nutzen, um die virtuellen Maschinen zu starten und zu stoppen. Wenn Sie dagegen **virsh** zum Starten der Maschine nutzen, kann es passieren, dass die virtuelle Maschine an mehr als einem Ort ausgeführt wird, was wiederum zur Beschädigung von Daten in der virtuellen Maschine führen kann.

Um die Wahrscheinlichkeit zu verringern, dass Administratoren versehentlich virtuelle Maschinen unter Verwendung von sowohl Cluster- als auch nicht-Cluster-Tools in einer Cluster-Umgebung "Doppel-Starten", können Sie die Konfigurationsdateien der virtuellen Maschine in einem nicht standardmäßigen Speicherort ablegen. Sind die Konfigurationsdateien der virtuellen Maschine an einem ungewöhnlichen Speicherort abgelegt, ist der versehentliche Start der virtuellen Maschine mit **virsh** erschwert, da die Konfigurationsdateien für **virsh** unbekannt sein werden.

Dieser nicht standardmäßige Speicherort für die Konfigurationsdateien der virtuellen Maschine kann sich an einem beliebigen Ort befinden. Der Vorteil bei der Verwendung einer NFS-Freigabe oder eines gemeinsam verwendeten GFS2-Dateisystems besteht darin, dass der Administrator die Konfigurationsdateien nicht auf allen Cluster-Mitgliedern synchronisieren muss. Es ist jedoch auch möglich, ein lokales Verzeichnis zu verwenden, vorausgesetzt der Administrator kann dessen Inhalte im gesamten Cluster synchron halten.

In der Cluster-Konfiguration können virtuelle Maschinen diesen nicht standardmäßigen Speicherort mithilfe des **path** Parameters einer virtuellen Maschinen-Ressource referenzieren. Beachten Sie, dass der **path** Parameter ein Verzeichnis oder eine Reihe von Verzeichnissen (getrennt durch das ':' Zeichen) spezifiziert, keinen Pfad zu einer bestimmten Datei.



Warnung

Der **`libvirt-guests`** Dienst sollte auf allen Knoten, auf denen **`rgmanager`** ausgeführt wird, deaktiviert werden. Falls eine virtuelle Maschine automatisch startet oder fortgeführt wird, kann es passieren, dass die virtuelle Maschine an mehr als einem Ort läuft, was wiederum zur Beschädigung von Daten in der virtuellen Maschine führen kann.

Für Informationen über die Parameter von virtuellen Maschinen-Ressourcen siehe Tabelle B.24, „Virtuelle Maschine (**`vm`**-Ressource)“.

Kapitel 3. Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Conga

Dieses Kapitel beschreibt die Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software mittels **Conga**. Informationen über die Verwendung von **Conga** zur Verwaltung eines laufenden Clusters finden Sie in Kapitel 4, *Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit **Conga***.



Anmerkung

Conga ist eine grafische Benutzeroberfläche, mithilfe derer Sie das Red Hat Hochverfügbarkeits-Add-On verwalten können. Beachten Sie jedoch, dass Sie ein umfassend gutes Verständnis der zugrunde liegenden Konzepte haben sollten, um diese Oberfläche effektiv einsetzen zu können. Wir raten Ihnen davon ab, sich das Wissen über Cluster-Konfiguration durch simples Ausprobieren der verfügbaren Features der Benutzeroberfläche anzueignen, da dies ein System zur Folge haben könnte, das nicht stabil genug ist, um auch im Falle von ausgefallenen Komponenten alle Dienste am Laufen zu erhalten.

Dieses Kapitel umfasst die folgenden Abschnitte:

- Abschnitt 3.1, „Konfigurationsaufgaben“
- Abschnitt 3.2, „Starten von **luci** “
- Abschnitt 3.3, „Zugriffskontrolle für luci“
- Abschnitt 3.4, „Erstellen eines Clusters“
- Abschnitt 3.5, „Globale Cluster-Eigenschaften“
- Abschnitt 3.6, „Konfiguration von Fencing-Geräten“
- Abschnitt 3.7, „Konfiguration des Fencings für Cluster-Mitglieder“
- Abschnitt 3.8, „Konfiguration einer Ausfallsicherungs-Domain“
- Abschnitt 3.9, „Konfiguration von globalen Cluster-Eigenschaften“
- Abschnitt 3.10, „Hinzufügen eines Cluster-Dienstes zum Cluster“

3.1. Konfigurationsaufgaben

Zur Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software mit **Conga** gehören die folgenden Schritte:

1. Konfiguration und Ausführen der **Conga** Konfigurationsoberfläche — des **luci** Servers. Siehe Abschnitt 3.2, „Starten von **luci** “.
2. Erstellen eines Clusters. Siehe Abschnitt 3.4, „Erstellen eines Clusters“.
3. Konfiguration von globalen Cluster-Eigenschaften. Siehe Abschnitt 3.5, „Globale Cluster-Eigenschaften“.
4. Konfiguration von Fencing-Geräten. Siehe Abschnitt 3.6, „Konfiguration von Fencing-Geräten“.
5. Konfiguration von Fencing für Cluster-Mitglieder. Siehe Abschnitt 3.7, „Konfiguration des Fencings für Cluster-Mitglieder“.
6. Erstellen von Ausfallsicherungs-Domains. Siehe Abschnitt 3.8, „Konfiguration einer Ausfallsicherungs-Domain“.
7. Erstellen von Ressourcen. Siehe Abschnitt 3.9, „Konfiguration von globalen Cluster-Eigenschaften“.
8. Erstellen von Cluster-Diensten. Siehe Abschnitt 3.10, „Hinzufügen eines Cluster-Dienstes zum Cluster“.

3.2. Starten von luci



Installation von ricci

Um **luci** zur Konfiguration eines Clusters einsetzen zu können, muss **ricci** auf den Cluster-Knoten installiert sein und laufen, wie in Abschnitt 2.13, „Überlegungen zu **ricci**“ beschrieben. Wie in diesem Abschnitt beschrieben, erfordert die Verwendung von **ricci** ein Passwort. **luci** fordert Sie bei der Erstellung eines Clusters für jeden Cluster-Knoten zur Eingabe dieses Passworts auf, wie in Abschnitt 3.4, „Erstellen eines Clusters“ beschrieben.
Vergewissern Sie sich vor dem Start von **luci**, dass die IP-Ports auf allen Cluster-Knoten, mit denen **luci** kommunizieren wird, Verbindungen zu Port 11111 vom **luci** Server erlauben. Siehe Abschnitt 2.3.1, „Aktivieren von IP-Ports auf Cluster-Knoten“ für Informationen über das Aktivieren von IP-Ports auf Cluster-Knoten.

Um das Red Hat Hochverfügbarkeits-Add-On mit **Conga** zu verwalten, installieren und starten Sie **luci** wie folgt:

1. Wählen Sie einen Computer, der **luci** hosten soll, und installieren Sie die **luci** Software auf diesem Computer. Zum Beispiel:

```
# yum install luci
```



Anmerkung

In der Regel wird **luci** von einem Computer in einem Server-Käfig oder Rechenzentrum gehostet, aber auch ein Cluster-Computer kann **luci** hosten.

2. Starten Sie **luci** mittels **service luci start**. Zum Beispiel:

```
# service luci start
Starting luci: generating https SSL certificates...  done
                                                           [  OK  ]

Please, point your web browser to https://nano-01:8084 to access luci
```



Anmerkung

Ab der Red Hat Enterprise Linux 6.1 Release können Sie einige Verhaltensweisen von **luci** konfigurieren, indem Sie die **/etc/sysconfig/luci** Datei bearbeiten. Dazu gehören die Port- und Host-Parameter wie in Abschnitt 2.4, „Konfiguration von **luci** mithilfe von **/etc/sysconfig/luci**“ beschrieben. Veränderte Port- und Host-Parameter werden automatisch in der URL widergespiegelt, wenn der **luci** Dienst startet.

3. Geben Sie in einem Webbrowser die URL des **luci** Servers in das Adressfeld ein und klicken auf **Go** (oder ähnlich). Die URL-Syntax für den **luci** Server ist **https://*luci_server_hostname*:*luci_server_port***. Der Standardwert für ***luci_server_port*** ist **8084**.

   Beim ersten Zugriff auf **luci** wird eine Eingabeaufforderung hinsichtlich des selbst signierten SSL-Zertifikats (des **luci** Servers) angezeigt. Nach Bestätigung dieser Dialogfelder zeigt Ihr Webbrowser nun die **luci** Anmeldeseite.

4. Jeder Benutzer, der sich auf dem System, das **luci** hostet, anmelden kann, kann sich auch bei **luci** anmelden. Ab Red Hat Enterprise Linux 6.2 jedoch kann nur der Root-Benutzer auf dem System, das **luci** ausführt, auf die **luci** Komponenten zugreifen, bis ein Administrator (der Root-Benutzer oder ein anderer Benutzer mit Administratorrechten) die Berechtigungen für diesen

Benutzer erstellt. Für Informationen über das Erstellen von **luci** Berechtigungen für Benutzer werfen Sie einen Blick auf Abschnitt 3.3, „Zugriffskontrolle für luci“.

Nach erfolgreicher Anmeldung zeigt **luci** die **luci Homebase** Seite, wie in Abbildung 3.1, „luci Homebase-Seite“ dargestellt.

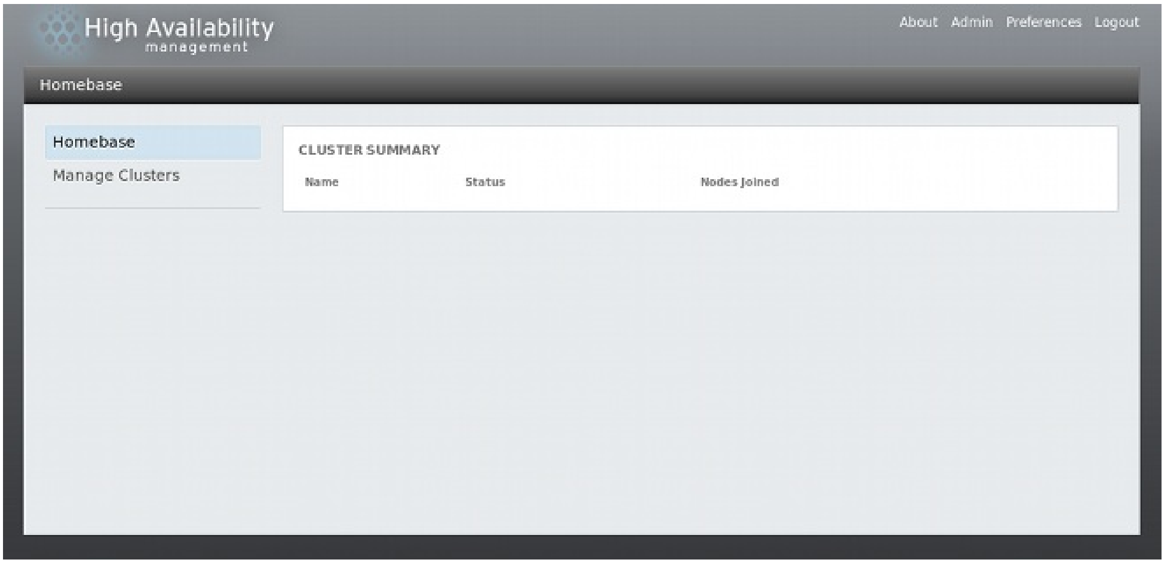


Abbildung 3.1. luci Homebase-Seite



Anmerkung

Nach 15 Minuten Inaktivität werden Sie automatisch aus **luci** abgemeldet.

3.3. Zugriffskontrolle für luci

Seit der ersten Version von Red Hat Enterprise Linux 6 wurden die folgenden Features zu der Seite **Users and Permisions** (Benutzer und Berechtigungen) hinzugefügt.

- Ab Red Hat Enterprise Linux 6.2 kann der Root-Benutzer oder ein Benutzer mit **luci** Administratorrechten auf einem System mit **luci** den Zugriff auf die verschiedenen **luci** Komponenten durch das Festlegen von Berechtigungen für die einzelnen Benutzer auf einem System kontrollieren.
- Ab Red Hat Enterprise Linux 6.3 kann der Root-Benutzer oder ein Benutzer mit **luci** Administratorrechten Benutzer zur **luci** Oberfläche hinzufügen und Berechtigungen für diesen Benutzer festlegen. Sie müssen diesen Benutzer nach wie vor noch zum System hinzufügen und ein Passwort festlegen, doch dieses Feature ermöglicht es Ihnen, Berechtigungen für diesen Benutzer festzulegen, bevor dieser sich zum ersten Mal bei **luci** anmeldet.
- Ab Red Hat Enterprise Linux 6.4 kann der Root-Benutzer oder ein Benutzer mit **luci** Administratorrechten auch die **luci** Oberfläche nutzen, um Benutzer von der **luci** Oberfläche zu entfernen, wodurch sämtliche Berechtigungen dieses Benutzers zurückgesetzt werden.



Anmerkung

Sie können die Art und Weise, wie **luci** Authentifizierung durchführt, ändern, indem Sie die **`/etc/pam.d/luci`** Datei auf dem System bearbeiten. Informationen über die Verwendung von Linux-PAM finden Sie auf der **`pam`**(8) Handbuchseite.

Um Benutzer hinzuzufügen, Benutzer zu löschen, oder die Benutzerrechte festzulegen, melden Sie sich

auf **luci** als **root** oder als Benutzer, dem zuvor Administratorrechte erteilt wurden, und klicken Sie auf die **Admin** Auswahl in der oberen rechten Ecke des **luci** Bildschirmes. Dies ruft die Seite **Users and Permissions** (Benutzer und Berechtigungen) auf, welche die vorhandenen Benutzer anzeigt.

Um einen Benutzer zur **luci** Oberfläche hinzuzufügen, klicken Sie auf **Add a User** (Benutzer hinzufügen) und geben Sie den Namen des Benutzers ein, den Sie hinzufügen möchten. Anschließend können Sie Berechtigungen für diesen Benutzer einstellen, allerdings müssen Sie auch noch ein Passwort für diesen Benutzer festlegen.

Um Benutzer von der **luci** Oberfläche zu löschen und sämtliche Berechtigungen für diesen Benutzer zurückzusetzen, wählen Sie den Benutzer oder mehrere aus und klicken Sie auf **Delete Selected** (Auswahl löschen).

Zum Erstellen oder Ändern von Berechtigungen für einen Benutzer wählen Sie den Benutzer aus dem Dropdown-Menü unter **User Permissions** (Benutzerberechtigungen). Dies ermöglicht es Ihnen, die folgenden Berechtigungen festzulegen:

Luci Administrator

Gewährt dem Benutzer dieselben Berechtigungen wie der Root-Benutzer, einschließlich umfassender Berechtigungen auf allen Clustern und der Fähigkeit, Berechtigungen auf allen anderen Benutzern zu verändern mit Ausnahme vom Root-Benutzer, dessen Berechtigungen nicht eingeschränkt werden können.

Can Create Clusters (Kann Cluster erstellen)

Erlaubt es dem Benutzer, neue Cluster zu erstellen, wie in Abschnitt 3.4, „Erstellen eines Clusters“ beschrieben.

Can Import Existing Clusters (Kann vorhandene Cluster importieren)

Erlaubt es dem Benutzer, einen vorhandenen Cluster zur **luci** Oberfläche hinzuzufügen, wie in Abschnitt 4.1, „Hinzufügen eines vorhandenen Clusters zur luci-Oberfläche“ beschrieben.

Für jeden Cluster, der in **luci** erstellt oder importiert wurde, können Sie die folgenden Berechtigungen für den angegebenen Benutzer festlegen:

Can View This Cluster (Kann diesen Cluster ansehen)

Erlaubt es dem Benutzer, den angegebenen Cluster anzusehen.

Can Change the Cluster Configuration (Kann die Cluster-Konfiguration ändern)

Erlaubt es dem Benutzer, die Konfiguration für den angegebenen Cluster zu ändern; davon ausgenommen ist das Hinzufügen und Entfernen von Cluster-Knoten.

Can Enable, Disable, Relocate, and Migrate Service Groups (Kann Dienstgruppen aktivieren, deaktivieren, verlegen und migrieren)

Erlaubt es dem Benutzer, Hochverfügbarkeitsdienste zu verwalten, wie in Abschnitt 4.5, „Verwaltung von Hochverfügbarkeitsdiensten“ beschrieben.

Can Stop, Start, and Reboot Cluster Nodes (Kann Cluster-Knoten stoppen, starten und neu starten)

Erlaubt es dem Benutzer, die einzelnen Knoten eines Clusters zu verwalten, wie in Abschnitt 4.3, „Verwaltung von Cluster-Knoten“ beschrieben.

Can Add and Delete Nodes (Kann Knoten hinzufügen und entfernen)

Erlaubt es dem Benutzer, Knoten zu einem Cluster hinzuzufügen oder davon zu entfernen, wie in Abschnitt 3.4, „Erstellen eines Clusters“ beschrieben.

`Can Remove This Cluster from Luci` (Kann diesen Cluster aus Luci entfernen)

Erlaubt es dem Benutzer, einen Cluster aus der **luci** Oberfläche zu entfernen, wie in Abschnitt 4.4, „Starten, Stoppen, Neustarten und Löschen von Clustern“ beschrieben.

Klicken Sie auf **`Submit`** (Einreichen), damit die Berechtigungen wirksam werden, oder klicken Sie auf **`Reset`** (Zurücksetzen), um zu den ursprünglichen Werten zurückzukehren.

3.4. Erstellen eines Clusters

Zum Erstellen eines Clusters mit **luci** gehört das Benennen des Clusters, das Hinzufügen von Knoten zum Cluster, Eingabe ihrer jeweiligen **ricci** Passwörter, und Abschicken der Anforderung zur Cluster-Erstellung. Sind die Knotenangaben und Passwörter korrekt, installiert **Conga** automatisch Software auf den Cluster-Knoten (sofern die richtigen Software-Pakete nicht bereits installiert sind) und startet den Cluster. Erstellen Sie einen Cluster wie folgt:

1. Klicken Sie auf **Manage Clusters** (Cluster verwalten) im Menü auf der linken Seite der **luci Homebase** Seite. Der **Clusters** Bildschirm erscheint, wie in Abbildung 3.2, „luci-Seite zur Cluster-Verwaltung“ dargestellt.

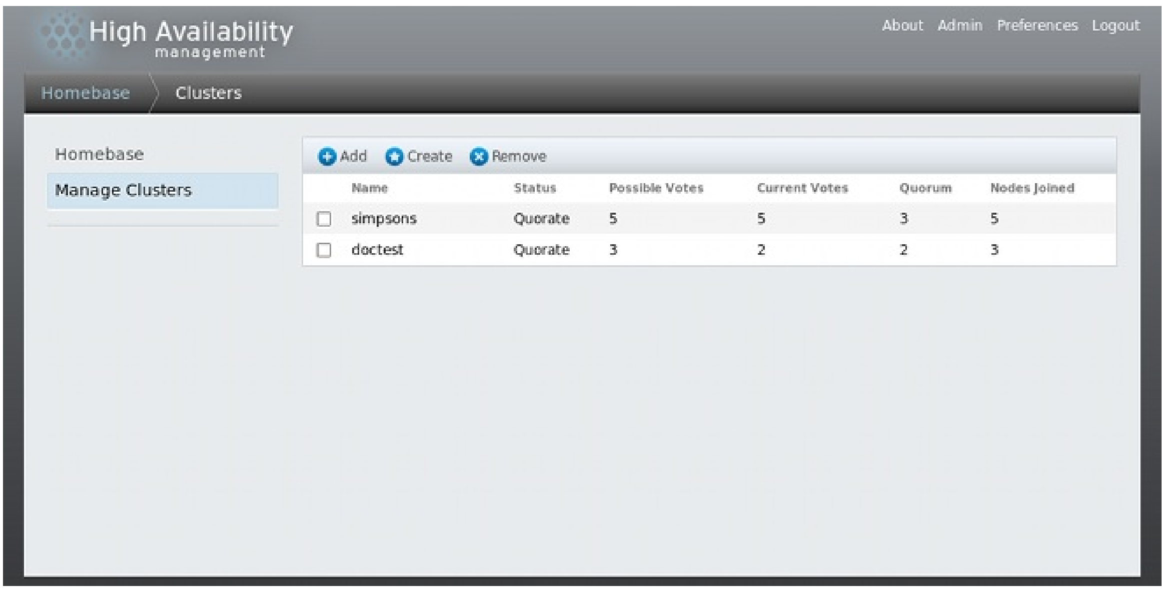


Abbildung 3.2. luci-Seite zur Cluster-Verwaltung

2. Klicken Sie auf **Create** (Erstellen). Der Bildschirm **Create New Cluster** (Neuen Cluster erstellen) erscheint, wie in Abbildung 3.3, „luci-Dialogfeld zur Cluster-Erstellung“ dargestellt.

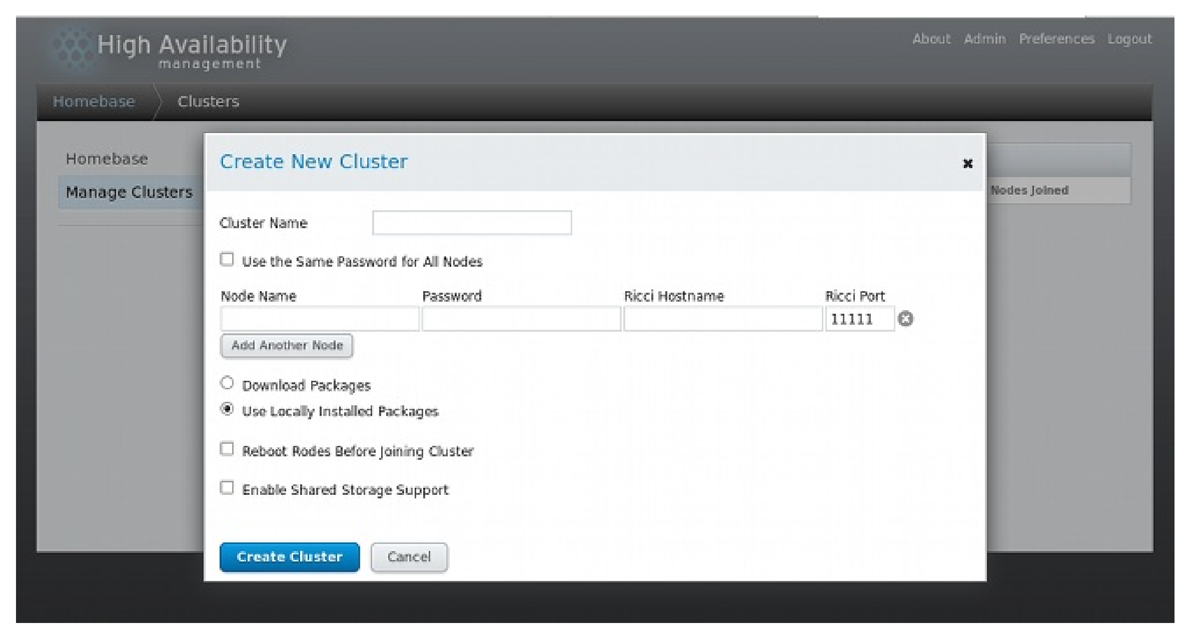


Abbildung 3.3. luci-Dialogfeld zur Cluster-Erstellung

3. Geben Sie im Dialogfeld **Create New Cluster** die folgenden Parameter ein:
   - Geben Sie im Textfeld **Cluster Name** einen Cluster-Namen ein. Der Cluster-Name darf nicht länger als 15 Zeichen sein.
   - Falls alle Knoten im Cluster dasselbe **ricci** Passwort haben, können Sie das Auswahlkästchen **Use the same password for all nodes** (Dasselbe Passwort für alle Knoten verwenden) markieren, um beim Hinzufügen weiterer Knoten das **password** Feld automatisch auszufüllen.
   - Geben Sie in der Spalte **Node Name** den Knotennamen für einen Knoten im Cluster ein und geben Sie das **ricci** Passwort für den Knoten in der **Password** Spalte ein. Ein Knotenname darf maximal 255 Bytes lang sein.
   - Falls Ihr System mit einem dedizierten privaten Netzwerk konfiguriert ist, das ausschließlich für Cluster-Datenverkehr genutzt wird, können Sie **luci** dahingehend konfigurieren, dass die Kommunikation mit **ricci** auf einer Adresse erfolgt, die sich von der Adresse unterscheidet, in die der Cluster-Knotenname aufgelöst wird. Sie erreichen dies, indem Sie diese Adresse als **Ricci Hostname** festlegen.
   - Falls Sie einen anderen Port für den **ricci** Agenten als den Standard 11111 verwenden, können Sie diesen Parameter hier ändern.
   - Klicken Sie auf **Add Another Node** (Weiteren Knoten hinzufügen) und geben Sie den Knotennamen und das **ricci** Passwort für jeden weiteren Knoten im Cluster ein.
   - Falls Sie beim Erstellen des Clusters nicht die bereits auf den Knoten installierten Cluster-Software-Pakete aktualisieren möchten, lassen Sie die Option **Use locally installed packages** (Lokal installierte Pakete verwenden) ausgewählt. Falls Sie dagegen alle Cluster-Software-Pakete aktualisieren möchten, wählen Sie die Option **Download Packages** (Pakete herunterladen).

     Anmerkung

     Ungeachtet dessen, ob Sie die Option **Use locally installed packages** oder **Download Packages** wählen, werden eventuell fehlende Basis-Cluster-Komponenten (**`cman`**, **`rgmanager`**, **`modcluster`** samt Abhängigkeiten) installiert. Falls diese nicht installiert werden können, wird die Knotenerstellung misslingen.

   - Wählen Sie **Reboot nodes before joining cluster** (Knoten vor Cluster-Beitritt neu starten) falls gewünscht.

- Wählen Sie **Enable shared storage support** (Unterstützung für gemeinsam verwendeten Speicher aktivieren), falls geclusterter Speicher erforderlich ist; dadurch werden die Pakete heruntergeladen, die Unterstützung für geclusterten Speicher hinzufügen, und geclustertes LVM wird aktiviert. Sie sollten dies nur dann auswählen, wenn Sie Zugriff auf das Resilient Storage Add-On oder das Scalable File System Add-On haben.

4. Klicken Sie auf **`Create Cluster`** (Cluster erstellen). Der Klick auf **`Create Cluster`** löst die folgenden Aktionen aus:

   a. Falls Sie **Download Packages** (Pakete herunterladen) ausgewählt haben, werden die Cluster-Software-Pakete auf die Knoten heruntergeladen.

   b. Cluster-Software wird auf den Knoten installiert (bzw. es wird überprüft, ob die richtigen Software-Pakete installiert sind).

   c. Die Cluster-Konfigurationsdatei wird aktualisiert und an jeden Knoten im Cluster weitergereicht.

   d. Die hinzugefügten Knoten treten dem Cluster bei.

   Eine Meldung wird angezeigt, die besagt, dass der Cluster derzeit erstellt wird. Sobald der Cluster bereit ist, wird der Status des neu erstellten Clusters angezeigt, wie in Abbildung 3.4, „Anzeige der Cluster-Knoten“ dargestellt. Beachten Sie, dass die Cluster-Erstellung fehlschlagen wird, wenn **ricci** auf keinem der Knoten ausgeführt wird.

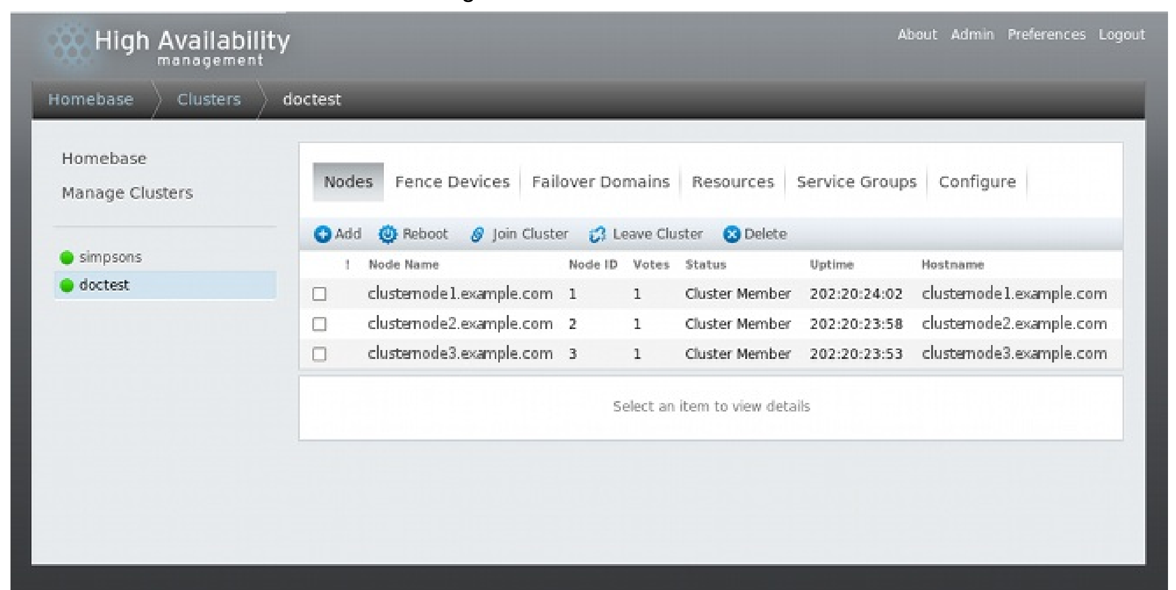


Abbildung 3.4. Anzeige der Cluster-Knoten

5. Nachdem Sie auf **`Create Cluster`** geklickt haben, um den Cluster zu erstellen, können Sie weitere Knoten zum Cluster hinzufügen oder Knoten aus ihm entfernen, indem Sie auf die **Add** (Hinzufügen) oder **Delete** (Löschen) Funktion oben auf der Cluster-Knoten-Ansichtsseite klicken. Vor dem Löschen von Knoten müssen diese gestoppt werden, es sei denn, Sie löschen den gesamten Cluster. Weitere Informationen über das Löschen eines Knotens aus einem laufenden Cluster finden Sie in Abschnitt 4.3.4, „Ein Mitglied aus einem Cluster löschen“.



Anmerkung

Das Entfernen eines Cluster-Knotens von einem Cluster ist eine destruktive Operation, die nicht rückgängig gemacht werden kann.

3.5. Globale Cluster-Eigenschaften

Wenn Sie einen Cluster zum Konfigurieren auswählen, wird eine clusterspezifische Seite angezeigt. Die Seite zeigt eine Oberfläche zur Konfiguration von clusterweiten Eigenschaften. Sie können clusterweite

Eigenschaften konfigurieren, indem Sie auf **Configure** oben in der Cluster-Anzeige klicken. Daraufhin wird eine Seite angezeigt mit den folgenden Reitern: **General**, **Fence Daemon**, **Network**, **Redundant Ring**, **QDisk** und **Logging**. Um die Parameter auf den Reitern zu konfigurieren, folgen Sie den Schritten in den folgenden Abschnitten. Wenn Sie einen Parameter auf einem Reiter nicht zu konfigurieren brauchen, überspringen Sie den Abschnitt für diesen Reiter.

3.5.1. Konfiguration der allgemeinen Eigenschaften

Ein Klick auf den **General** Reiter zeigt die **General Properties** (Allgemeine Eigenschaften) Seite, die eine Oberfläche zur Änderung der Konfigurationsversion bietet.

- Das Textfeld **Cluster Name** zeigt den Cluster-Namen, es akzeptiert jedoch keine Änderung des Cluster-Namens. Die einzige Möglichkeit, den Namen eines Clusters zu ändern, ist das Erstellen einer neuen Cluster-Konfiguration mit dem neuen Namen.
- Der Wert für die **Configuration Version** (Konfigurationsversion) ist standardmäßig auf **1** gesetzt und wird jedes Mal automatisch erhöht, wenn Sie Ihre Cluster-Konfiguration ändern. Falls Sie jedoch einen abweichenden Wert angeben müssen, können Sie diesen manuell im Textfeld **Configuration Version** angeben.

Falls Sie den **Configuration Version** Wert verändert haben, klicken Sie auf **`Apply`** (Anwenden), damit diese Änderung wirksam wird.

3.5.2. Konfiguration der Fencing-Daemon Eigenschaften

Ein Klick auf den **Fence Daemon** Reiter zeigt die **Fence Daemon Properties** (Fencing-Daemon Eigenschaften) Seite, die eine Oberfläche zur Konfiguration von **Post Fail Delay** und **Post Join Delay** bietet. Die Werte, die Sie für diese Parameter erstellen, sind allgemeine Fencing-Eigenschaften für den gesamten Cluster. Um bestimmte Fencing-Geräte für Knoten im Cluster zu konfigurieren, verwenden Sie den Menüpunkt **Fence Devices** (Fencing-Geräte) in der Cluster-Anzeige, wie in Abschnitt 3.6, „Konfiguration von Fencing-Geräten“ beschrieben.

- Der Parameter **Post Fail Delay** (Verzögerung nach Ausfall) ist die Anzahl von Sekunden, die der Fencing-Daemon (**`fenced`**) wartet, bevor ein Knoten (ein Mitglied der Fencing-Domain) nach dessen Ausfall abgegrenzt wird. Der Standardwert für **Post Fail Delay** ist **`0`**. Dieser Wert kann je nach Cluster- und Netzwerkleistung angepasst werden.
- Der Parameter **Post Join Delay** (Verzögerung nach Beitritt) ist die Anzahl der Sekunden, die der Fencing-Daemon (**`fenced`**) wartet, bevor ein Knoten abgegrenzt wird, nachdem der Knoten der Fencing-Domain beitritt. **luci** setzt den **Post Join Delay** Wert standardmäßig auf **3**. Eine typische Einstellung für **Post Join Delay** liegt zwischen 20 und 30 Sekunden, kann aber je nach Cluster- und Netzwerkleistung variieren.

Geben Sie die erforderlichen Werte ein und klicken auf **`Apply`** (anwenden), damit diese Änderungen wirksam werden.



Anmerkung

Weitere Informationen über **Post Join Delay** und **Post Fail Delay** finden Sie auf der fenced(8) Handbuchseite.

3.5.3. Konfiguration des Netzwerks

Ein Klick auf den **Network** Reiter zeigt die **Network Configuration** Seite, die eine Oberfläche zur Konfiguration des Netzwerktransporttyps bietet.

Sie können auf diesem Reiter eine der folgenden Optionen wählen:

- **UDP Multicast and Let Cluster Choose the Multicast Address** (UDP-Multicast und den Cluster die Multicast-Adresse auswählen lassen)

Dies ist die Standardeinstellung. Wenn Sie diese Option auswählen, erstellt die Red Hat Hochverfügbarkeits-Add-On-Software eine Multicast-Adresse basierend auf der Cluster-ID. Es generiert die unteren 16 Bits der Adresse und fügt diese an den oberen Teil der Adresse an, abhängig davon, ob das IP-Protokoll IPv4 oder IPv6 verwendet wird:

- Bei IPv4 — Die gebildete Adresse ist 239.192. plus die von der Red Hat Hochverfügbarkeits-Add-On-Software generierten unteren 16 Bits.
- Bei IPv6 — Die gebildete Adresse ist FF15:: plus die von der Red Hat Hochverfügbarkeits-Add-On-Software generierten unteren 16 Bits.



Anmerkung

Die Cluster-ID ist eine eindeutige Kennung, die **`cman`** für jeden Cluster generiert. Um die Cluster-ID anzusehen, führen Sie den **`cman_tool status`** Befehl auf einem Cluster-Knoten durch.

- **UDP Multicast and Specify the Multicast Address Manually** (UDP-Multicast und manuell die Multicast-Adresse angeben)

  Falls Sie eine bestimmte Multicast-Adresse verwenden müssen, wählen Sie diese Option und geben Sie im Textfeld **Multicast Address** eine Multicast-Adresse an.

  Falls Sie eine Multicast-Adresse angeben, sollten Sie die 239.192.x.x Serie (oder FF15:: für IPv6) nutzen, die **`cman`** verwendet. Falls Sie eine Multicast-Adresse außerhalb dieses Bereichs verwenden, kann dies eventuell zu unvorhergesehenem Verhalten führen. So könnte z.B. die Adresse 224.0.0.x (d.h. "Alle Hosts auf dem Netzwerk") unter Umständen von mancher Hardware nicht korrekt oder gar nicht geroutet werden.

  Falls Sie eine Multicast-Adresse angeben oder ändern, müssen Sie den Cluster-Knoten neu starten, damit die Änderungen wirksam werden. Für Informationen über das Starten und Stoppen eines Clusters mit **Conga** siehe Abschnitt 4.4, „Starten, Stoppen, Neustarten und Löschen von Clustern“.



Anmerkung

Falls Sie eine Multicast-Adresse angeben, überprüfen Sie die Konfiguration der Router, die von Cluster-Paketen durchquert werden. Manche Router brauchen eine lange Zeit zum Lernen von Adressen, was sich drastisch auf die Cluster-Leistung auswirken kann.

- **UDP Unicast (UDPU)**

  Ab der Red Hat Enterprise Linux 6.2 Release können die Knoten in einem Cluster miteinander über den UDP-Unicast Transportmechanismus kommunizieren. Es wird jedoch empfohlen, dass Sie IP-Multicasting für das Cluster-Netzwerk verwenden. UDP-Unicast ist eine Alternative, die verwendet werden kann, wenn IP-Multicasting nicht zur Verfügung steht. Für GFS2-Bereitstellungen wird die Verwendung von UDP Unicast nicht empfohlen.

Klicken Sie auf **`Apply`** (Anwenden). Wenn Sie den Transporttyp ändern, ist ein Neustart des Clusters nötig, damit die Änderungen wirksam werden.

3.5.4. Konfiguration des Redundant Ring Protocols

Ab Red Hat Enterprise Linux 6.4 unterstützt das Red Hat Hochverfügbarkeits-Add-On die Konfiguration des Redundant Ring Protocols. Bei der Verwendung des Redundant Ring Protocols müssen Sie eine Vielzahl von Überlegungen berücksichtigen, wie in Abschnitt 7.6, „Konfiguration von Redundant Ring Protocol“ beschrieben.

Ein Klick auf den **Redundant Ring** Reiter zeigt die **Redundant Ring Protocol Configuration** Seite an. Auf dieser Seite werden alle Knoten angezeigt, die aktuell für den Cluster konfiguriert sind. Wenn Sie ein System zur Verwendung des Redundant Ring Protocols konfigurieren, müssen Sie den **Alternate Name** für jeden Knoten für den zweiten Ring angeben.

Mit der **Redundant Ring Protocol Configuration** Seite können Sie optional die **Alternate Ring Multicast Address**, den **Alternate Ring CMAN Port** und die **Alternate Ring Multicast Packet TTL** für den zweiten Ring festlegen.

Wenn Sie eine Multicast-Adresse für den zweiten Ring angeben, muss entweder die alternative Multicast-Adresse oder der alternative Port anders sein als die Multicast-Adresse für den ersten Ring. Wenn Sie einen alternativen Port angeben, müssen die Port-Nummern des ersten Rings und des zweiten Rings um mindestens zwei unterschiedlich sein, da das System selbst port und port-1 verwendet, um Operationen durchzuführen. Wenn Sie keine alternative Multicast-Adresse angeben haben, wird das System automatisch eine andere Multicast-Adresse für den zweiten Ring verwenden.

3.5.5. Konfiguration des Quorumdatenträgers

Ein Klick auf den **QDisk** Reiter zeigt die **Quorum Disk Configuration** Seite, die eine Oberfläche zur Konfiguration von Quorumdatenträgerparametern bietet, falls Sie einen Quorumdatenträger verwenden müssen.



Wichtig

Die Parameter und Heuristiken des Quorumdatenträgers hängen von der jeweiligen Umgebung und ggf. besonderen Anforderungen ab. Um die Parameter und Heuristiken des Quorumdatenträgers zu verstehen, werfen Sie einen Blick auf die qdisk(5) Handbuchseite. Falls Sie Hilfe zum Verständnis oder zur Verwendung von Quorumdatenträgern benötigen, setzen Sie sich bitte mit einem autorisierten Red Hat Support-Vertreter in Verbindung.

Der Parameter **Do Not Use a Quorum Disk** (Keinen Quorumdatenträger verwenden) ist standardmäßig aktiviert. Wenn Sie einen Quorumdatenträger verwenden müssen, klicken Sie auf **Use a Quorum Disk** (Quorumdatenträger verwenden), geben Sie die Parameter des Quorum-Datenträgers an, klicken Sie auf **`Apply`** (Anwenden) und starten Sie den Cluster neu, damit die Änderungen wirksam werden.

Tabelle 3.1, „Parameter des Quorumdatenträgers“ beschreibt die Parameter des Quorumdatenträgers.

Tabelle 3.1. Parameter des Quorumdatenträgers

Parameter	Beschreibung
Specify Physical Device: By Device Label	Spezifiziert die Kennung des Quorumdatenträgers, das von dem **mkqdisk** Dienstprogramm erstellt wurde. Wird dieses Feld verwendet, liest der Quorum-Daemon die **/proc/partitions** Datei, sucht nach qdisk-Signaturen auf jedem gefundenen Blockgerät und vergleicht die Kennung mit der angegebenen Kennung. Dies ist in Konfigurationen hilfreich, in denen der Name des Quorumgeräts sich von Knoten zu Knoten unterscheidet.
Heuristics	**Path to Program** — Das Programm, das verwendet wird, um festzustellen, ob diese Heuristik verfügbar ist. Dies kann alles sein, was durch **/bin/sh-c** ausgeführt werden kann. Ein Rückgabewert von 0 bedeutet Erfolg, alles andere bedeutet Misserfolg. Dieses Feld ist erforderlich. **Interval** — Die Zeitabstände (in Sekunden), in denen die Heuristik abgefragt wird. Das standardmäßige Intervall für jede Heuristik ist 2 Sekunden. **Score** — Die Gewichtung dieser Heuristik. Seien Sie vorsichtig beim Festlegen der Gewichtung für Heuristiken. Die standardmäßige Gewichtung für jede Heuristik ist 1. **TKO** — Die Anzahl von aufeinander folgenden Fehlschlägen, bevor diese Heuristik für nicht verfügbar erklärt wird.
Minimum Total Score	Die Mindestpunktzahl eines Knotens, bei der dieser noch als "lebendig" betrachtet wird. Falls dieser Wert weggelassen oder auf 0 gesetzt wird, so wird die Standardfunktion **floor((*n*+1)/2)** verwendet, wobei ***n*** die Summe der Heuristik-Punktzahlen ist. Der **Minimum Total Score** Wert darf nie die Summe der Heuristik-Punktzahlen übersteigen, andernfalls wird der Quorumdatenträger nicht verfügbar sein.



Anmerkung

Durch einen Klick auf **Apply** auf dem Reiter **QDisk Configuration** werden die Änderungen in die Cluster-Konfigurationsdatei (**/etc/cluster/cluster.conf**) auf jedem Cluster-Knoten übertragen. Damit der Quorumdatenträger jedoch funktioniert und damit jegliche Änderungen an den Parametern des Quorumdatenträgers wirksam werden, müssen Sie den Cluster neu starten (siehe Abschnitt 4.4, „Starten, Stoppen, Neustarten und Löschen von Clustern“) und sichergehen, dass der **qdiskd** Daemon auf jedem Knoten neu gestartet wurde.

3.5.6. Konfiguration der Protokollierung

Ein Klick auf den **Logging** Reiter zeigt die **Logging Configuration** Seite, die eine Oberfläche zur Konfiguration der Protokollierungseinstellungen bietet.

Die folgenden Einstellungen können Sie für die globale Protokollierungskonfiguration festlegen:

- Wenn Sie **Log Debugging Messages** (Debugging-Nachrichten protokollieren) auswählen, werden Debugging-Nachrichten in der Protokolldatei gespeichert.
- Wenn Sie **Log Messages to Syslog** (Nachrichten nach syslog protokollieren) auswählen, werden Nachrichten mit **syslog** protokolliert. Sie können die **Syslog Message Facility** und die **Syslog Message Priority** auswählen. Die Einstellung **Syslog Message Priority** (Syslog-Nachrichtenpriorität) legt fest, dass Nachrichten mit der ausgewählten Priorität oder höher an

syslog gesendet werden.

- Wenn Sie **Log Messages to Log File** (Nachrichten in Protokolldatei speichern) auswählen, werden Nachrichten in der Protokolldatei gespeichert. Sie können den **Log File Path** (Pfad zur Protokolldatei) angeben. Die Einstellung **Logfile Message Prioity** legt fest, dass Nachrichten mit der ausgewählten Priorität oder höher in der Protokolldatei gespeichert werden.

Sie können die globalen Protokollierungseinstellungen für bestimmte Daemons außer Kraft setzen, indem Sie einen der Daemons auswählen, die unter der Überschrift **Daemon-specific Logging Overrides** (daemonspezifische Sondereinstellungen zur Protokollierung) unten auf der **Logging Configuration** Seite aufgeführt sind. Nachdem Sie den Daemon ausgewählt haben, können Sie auswählen, ob die Debugging-Nachrichten für diesen Daemon protokolliert werden sollen. Sie können auch **syslog** und Protokolldateieinstellungen für diesen Daemon vornehmen.

Klicken Sie auf **Apply**, damit die Änderungen an der Protokollierungskonfiguration wirksam werden.

3.6. Konfiguration von Fencing-Geräten

Die Konfiguration von Fencing-Geräten umfasst das Erstellen, Aktualisieren und Löschen von Fencing-Geräten für den Cluster. Sie müssen die Fencing-Geräte in einem Cluster konfigurieren, bevor Sie Fencing für die Knoten im Cluster konfigurieren können.

Zum Erstellen eines Fencing-Geräts gehört die Auswahl eines Typ für das Fencing-Gerät und die Eingabe der Parameter für das Fencing-Gerät (z.B. Name, IP-Adresse, Login und Passwort). Zum Aktualisieren eines Fencing-Geräts gehört die Auswahl eines vorhandenen Fencing-Geräts und das Ändern der Parametern für dieses Fencing-Gerät. Zum Löschen eines Fencing-Geräts gehört die Auswahl eines vorhandenen Fencing-Geräts und das Löschen desselben.



Anmerkung

Es wird empfohlen, für jeden Knoten mehrere Fencing-Mechanismen zu konfigurieren. Ein Fencing-Gerät kann aus verschiedenen Gründen ausfallen, beispielsweise aufgrund einer Netzwerkspaltung, eines Stromausfalls oder eines Problems mit dem Fencing-Gerät selbst. Die Konfiguration mehrerer Fencing-Mechanismen verringert die Wahrscheinlichkeit, dass der Ausfall eines Fencing-Geräts schwerwiegende Folgen hat.

Dieser Abschnitt beschreibt die Verfahren für die folgenden Aufgaben:

- Erstellen von Fencing-Geräten — Siehe Abschnitt 3.6.1, „Erstellen eines Fencing-Geräts“. Nachdem Sie ein Fencing-Gerät erstellt und benannt haben, können Sie die Fencing-Geräte für jeden Knoten im Cluster konfigurieren wie in Abschnitt 3.7, „Konfiguration des Fencings für Cluster-Mitglieder“ beschrieben.
- Aktualisieren von Fencing-Geräten — Siehe Abschnitt 3.6.2, „Ändern eines Fencing-Geräts“.
- Löschen von Fencing-Geräten — Siehe Abschnitt 3.6.3, „Löschen eines Fencing-Geräts“.

Auf der clusterspezifischen Seite können Sie Fencing-Geräte für diesen Cluster konfigurieren, indem Sie auf **Fence Devices** (Fencing-Geräte) oben in der Cluster-Anzeige klicken. Daraufhin werden die Fencing-Geräte für den Cluster angezeigt, sowie die folgenden Menüpunkte zur Konfiguration der Fencing-Geräte: **Add** (Hinzufügen) und **Delete** (Löschen). Dies ist der Ausgangspunkt für alle Verfahren, die in den folgenden Abschnitten beschrieben werden.



Anmerkung

Falls es sich hierbei um die anfängliche Cluster-Konfiguration handelt, wurden noch keine Fencing-Geräte erstellt, weshalb in diesem Fall keine Geräte angezeigt werden.

Abbildung 3.5, „luci-Seite zur Konfiguration von Fencing-Geräten“ zeigt den Konfigurationsbildschirm, bevor jegliche Fencing-Geräte erstellt wurden.

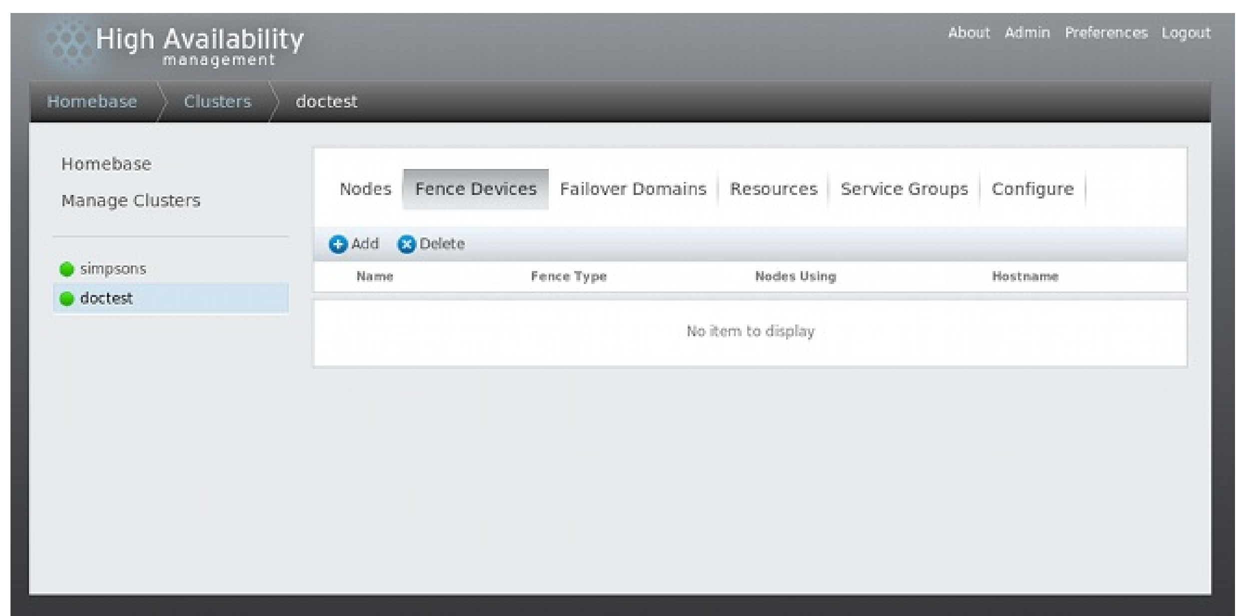


Abbildung 3.5. luci-Seite zur Konfiguration von Fencing-Geräten

3.6.1. Erstellen eines Fencing-Geräts

Um ein Fencing-Gerät zu erstellen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der **Fence Devices** Konfigurationsseite auf **Add** (Hinzufügen). Durch den Klick auf **Add** wird das Dialogfenster **Add Fence Device (Instance)** (Fencing-Geräteinstanz hinzufügen) angezeigt. Wählen Sie aus diesem Dialogfenster den Typ des zu konfigurierenden Fencing-Geräts.
2. Geben Sie die nötigen Informationen im Dialogfeld **Add Fence Device (Instance)** an, je nach Typ des Fencing-Geräts. Für weitere Informationen über Fencing-Geräteparameter siehe Anhang A, *Parameter der Fencing-Geräte*. In einigen Fällen müssen Sie zusätzliche, knotenspezifische Parameter für das Fencing-Gerät angeben, wenn Sie Fencing für individuelle Knoten konfigurieren, wie in Abschnitt 3.7, „Konfiguration des Fencings für Cluster-Mitglieder“ beschrieben.
3. Klicken Sie auf **Submit**.

Nachdem das Fencing-Gerät hinzugefügt wurde, erscheint sie auf der **Fence Devices** Konfigurationsseite.

3.6.2. Ändern eines Fencing-Geräts

Um ein Fencing-Gerät zu ändern, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der **Fence Devices** Konfigurationsseite auf den Namen des zu ändernden Fencing-Geräts. Dies öffnet ein Dialogfenster für dieses Fencing-Gerät, das die für dieses Gerät konfigurierten Werte anzeigt.
2. Um das Fencing-Gerät zu ändern, geben Sie die gewünschten Änderungen für die angezeigten Parameter ein. Siehe Anhang A, *Parameter der Fencing-Geräte* für weitere Informationen.
3. Klicken Sie auf **Apply** und warten Sie, bis die Konfiguration aktualisiert wurde.



Anmerkung

Fencing-Geräte, die derzeit in Gebrauch sind, können nicht gelöscht werden. Um ein Fencing-Gerät zu löschen, das derzeit in Gebrauch ist, aktualisieren Sie zunächst die Fencing-Konfiguration aller Knoten, die dieses Gerät verwenden, und löschen Sie anschließend das Gerät.

Um ein Fencing-Gerät zu löschen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der **Fence Devices** Konfigurationsseite das Auswahlkästchen links von den Fencing-Geräten, die Sie löschen möchten.
2. Klicken Sie auf **`Delete`** und warten Sie, bis die Konfiguration aktualisiert wurde. Es wird eine Meldung angezeigt, die bestätigt, welche Geräte gelöscht werden.

Sobald die Konfiguration aktualisiert wurde, erscheint das gelöschte Fencing-Gerät nicht länger in der Anzeige.

3.7. Konfiguration des Fencings für Cluster-Mitglieder

Nachdem Sie die ersten Schritte zum Erstellen eines Clusters und zum Erstellen von Fencing-Geräten abgeschlossen haben, müssen Sie nun das Fencing für die Cluster-Knoten konfigurieren. Um das Fencing für die Knoten zu konfigurieren, folgen Sie den Schritten in diesem Abschnitt. Beachten Sie, dass Sie das Fencing für jeden Knoten im Cluster konfigurieren müssen.

Die folgenden Abschnitte beschreiben das Verfahren zur Konfiguration eines einzelnen Fencing-Geräts für einen Knoten, zur Konfiguration eines Knotens mit einem Backup-Fencing-Gerät und zur Konfiguration eines Knotens mit redundanter Stromversorgung:

- Abschnitt 3.7.1, „Konfiguration eines einzelnen Fencing-Geräts für einen Knoten“
- Abschnitt 3.7.2, „Konfiguration eines Backup-Fencing-Geräts“
- Abschnitt 3.7.3, „Konfiguration eines Knotens mit redundanter Stromversorgung“

3.7.1. Konfiguration eines einzelnen Fencing-Geräts für einen Knoten

Nutzen Sie das folgende Verfahren, um einen Knoten mit einem einzelnen Fencing-Gerät zu konfigurieren.

1. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** (Knoten) oben in der Cluster-Anzeige, um Fencing für die Knoten im Cluster zu konfigurieren. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt. Dies ist zudem die Standardseite, die angezeigt wird, wenn Sie unter **Manage Clusters** im Menü auf der linken Seite der **luci Homebase** Seite auf den Cluster-Namen klicken.
2. Klicken Sie auf einen Knotennamen. Durch den Klick auf einen Link für einen Knoten erscheint eine Seite für diesen Link, auf der die Konfiguration für diesen Knoten angezeigt wird.

   Die knotenspezifische Seite zeigt alle Dienste an, die gegenwärtig auf dem Knoten laufen, sowie alle Ausfallsicherungs-Domains, bei denen der Knoten Mitglied ist. Sie können eine vorhandene Ausfallsicherungs-Domain ändern, indem Sie auf deren Namen klicken. Weitere Informationen über die Konfiguration von Ausfallsicherungs-Domains finden Sie in Abschnitt 3.8, „Konfiguration einer Ausfallsicherungs-Domain“.
3. Klicken Sie auf der knotenspezifischen Seite unter **Fence Devices** auf **`Add Fence Method`** (Fencing-Methode hinzufügen). Daraufhin wird das Dialogfenster **`Add Fence Method to Node`** (Fencing-Methode zum Knoten hinzufügen) angezeigt.
4. Geben Sie einen **Methode Name** (Methodennamen) für die Fencing-Methode ein, die Sie für diesen Knoten konfigurieren. Dies ist ein beliebiger Name, der von dem Red Hat Hochverfügbarkeits-Add-On verwendet wird; es handelt sich hierbei nicht um den DNS-Namen für das Gerät.

5. Klicken Sie auf **Submit**. Daraufhin wird der knotenspezifische Bildschirm angezeigt, der nun die Methode auflistet, die Sie eben unter **Fence Devices** hinzugefügt haben.
6. Konfigurieren Sie eine Fencing-Instanz für diese Methode, indem Sie auf die Schaltfläche **Add Fence Instance** (Fencing-Instanz hinzufügen) unter der Fencing-Methode klicken. Daraufhin wird das Drop-Down-Menü **Add Fence Device (Instance)** angezeigt, aus dem Sie ein Fencing-Gerät auswählen können, das Sie vorher wie in Abschnitt 3.6.1, „Erstellen eines Fencing-Geräts" beschrieben konfiguriert haben.
7. Wählen Sie ein Fencing-Gerät für diese Methode. Falls dieses Fencing-Gerät die Konfiguration von knotenspezifischen Parametern erfordert, werden die zu konfigurierenden Parameter angezeigt. Informationen über Fencing-Parameter finden Sie unter Anhang A, *Parameter der Fencing-Geräte*.



Anmerkung

Für andere Fencing-Methoden als das Power-Fencing (also SAN/Speicher-Fencing) ist auf der knotenspezifischen Parameteranzeige standardmäßig **Unfencing** ausgewählt. Dadurch wird sichergestellt, dass ein abgegrenzter Knoten erst dann wieder Zugriff auf den Datenspeicher hat, nachdem er neu gestartet wurde. Wenn Sie ein Gerät konfigurieren, dass Unfencing erfordert, muss der Cluster zunächst gestoppt werden, dann muss die vollständige Konfiguration einschließlich Geräte und Unfencing hinzugefügt werden, bevor der Cluster gestartet wird. Informationen über das Aufheben der Knotenabgrenzung finden Sie auf der **fence_node**(8) Handbuchseite.

8. Klicken Sie auf **Submit**. Daraufhin wird der knotenspezifische Bildschirm mit der Fencing-Methode und der Fencing-Instanz angezeigt.

3.7.2. Konfiguration eines Backup-Fencing-Geräts

Sie können mehrere Fencing-Methoden für einen Knoten definieren. Falls die Abgrenzung mit der ersten Methode fehlschlägt, wird das System versuchen, den Knoten mithilfe der zweiten Methode abzugrenzen, gefolgt von jeglichen zusätzlichen konfigurierten Methoden.

Nutzen Sie das folgende Verfahren, um ein Backup-Fencing-Gerät für einen Knoten zu konfigurieren.

1. Nutzen Sie das in Abschnitt 3.7.1, „Konfiguration eines einzelnen Fencing-Geräts für einen Knoten" beschriebene Verfahren, um die primäre Fencing-Methode für einen Knoten zu konfigurieren.
2. Klicken Sie unter der von Ihnen definierten primären Methode auf **Add Fence Method**.
3. Geben Sie einen Namen für die Backup-Fencing-Methode an, die Sie für diesen Knoten konfigurieren, und klicken Sie auf **Submit**. Daraufhin wird der knotenspezifische Bildschirm angezeigt, der unter der primären Fencing-Methode nun auch die eben von Ihnen hinzugefügte Methode anzeigt.
4. Konfigurieren Sie eine Fencing-Instanz für diese Methode, indem Sie auf **Add Fence Instance** (Fencing-Instanz hinzufügen) klicken. Daraufhin wird ein Drop-Down-Menü angezeigt, aus dem Sie ein Fencing-Gerät auswählen können, das Sie vorher wie in Abschnitt 3.6.1, „Erstellen eines Fencing-Geräts" beschrieben konfiguriert haben.
5. Wählen Sie ein Fencing-Gerät für diese Methode. Falls dieses Fencing-Gerät die Konfiguration von knotenspezifischen Parametern erfordert, werden die zu konfigurierenden Parameter angezeigt. Informationen über Fencing-Parameter finden Sie unter Anhang A, *Parameter der Fencing-Geräte*.
6. Klicken Sie auf **Submit**. Daraufhin wird der knotenspezifische Bildschirm mit der Fencing-Methode und der Fencing-Instanz angezeigt.

Bei Bedarf können Sie weitere Fencing-Methoden hinzufügen. Sie können die Reihenfolge ändern, in der die Fencing-Methoden für diesen Knoten verwendet werden, indem Sie auf **Move Up** und **Move Down** klicken.

3.7.3. Konfiguration eines Knotens mit redundanter Stromversorgung

Falls Ihr Cluster mit redundanter Stromversorgung für Ihre Knoten ausgestattet ist, vergewissern Sie sich, dass Ihr Fencing derart konfiguriert ist, dass Ihre Knoten bei der Abgrenzung vollständig abgeschaltet werden. Falls Sie jede Stromversorgung als separate Fencing-Methode konfigurieren, wird jede Stromversorgung separat abgegrenzt; die zweite Stromversorgung ermöglicht es dem System, weiterhin zu laufen, selbst wenn die erste Stromversorgung abgegrenzt ist, so dass das System selbst im Endeffekt nicht abgegrenzt wird. Um ein System mit dualer Stromversorgung zu konfigurieren, müssen Sie Ihre Fencing-Geräte so konfigurieren, dass beide Stromversorgungen abgeschaltet werden und somit auch das System vollständig abgeschaltet wird. Wenn Sie Ihr System mittels **Conga** konfigurieren, müssen Sie hierzu zwei Instanzen innerhalb einer einzelnen Fencing-Methode konfigurieren.

Um das Fencing für einen Knoten mit dualer Stromversorgung zu konfigurieren, folgen Sie den Schritten in diesem Abschnitt.

1. Bevor Sie das Fencing für einen Knoten mit redundanter Stromversorgung konfigurieren können, müssen Sie jeden der Netzschalter als Fencing-Gerät für den Cluster konfigurieren. Informationen über die Konfiguration von Fencing-Geräten finden Sie in Abschnitt 3.6, „Konfiguration von Fencing-Geräten“.
2. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** (Knoten) oben in der Cluster-Anzeige. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt. Dies ist zudem die Standardseite, die angezeigt wird, wenn Sie unter **Manage Clusters** im Menü auf der linken Seite der **luci Homebase** Seite auf den Cluster-Namen klicken.
3. Klicken Sie auf einen Knotennamen. Durch den Klick auf einen Link für einen Knoten erscheint eine Seite für diesen Link, auf der die Konfiguration für diesen Knoten angezeigt wird.
4. Klicken Sie auf der knotenspezifischen Seite auf **`Add Fence Method`** (Fencing-Methode hinzufügen).
5. Geben Sie einen Namen für die Fencing-Methode an, die Sie für diesen Knoten konfigurieren.
6. Klicken Sie auf **`Submit`**. Daraufhin wird der knotenspezifische Bildschirm angezeigt, der nun die Methode auflistet, die Sie eben unter **Fence Devices** hinzugefügt haben.
7. Konfigurieren Sie die erste Stromversorgung als eine Fencing-Instanz für diese Methode, indem Sie auf **`Add Fence Instance`** klicken. Daraufhin wird ein Drop-Down-Menü angezeigt, aus dem Sie eines der Power-Fencing-Geräte auswählen können, die Sie vorher konfiguriert haben, wie in Abschnitt 3.6.1, „Erstellen eines Fencing-Geräts“ beschrieben.
8. Wählen Sie eines der Power-Fencing-Geräte für diese Methode und geben die entsprechenden Parameter für dieses Gerät an.
9. Klicken Sie auf **`Submit`**. Daraufhin wird der knotenspezifische Bildschirm mit der Fencing-Methode und der Fencing-Instanz angezeigt.
10. Klicken Sie unter derselben Fencing-Methode, für die Sie das erste Power-Fencing-Gerät konfiguriert haben, auf **`Add Fence Instance`**. Daraufhin wird ein Drop-Down-Menü angezeigt, aus dem Sie das zweite Power-Fencing-Gerät auswählen können, die Sie vorher wie in Abschnitt 3.6.1, „Erstellen eines Fencing-Geräts“ beschrieben konfiguriert haben.
11. Wählen Sie das zweite Power-Fencing-Gerät für diese Methode und geben die entsprechenden Parameter für dieses Gerät an.
12. Klicken Sie auf **`Submit`**. Dadurch kehren Sie zum knotenspezifischen Bildschirm mit den Fencing-Methoden und Fencing-Instanzen zurück, der nun anzeigt, dass jedes Gerät das System in der angegebenen Reihenfolge abschaltet und in der angegebenen Reihenfolge wieder einschaltet. Dies wird in Abbildung 3.6, „Fencing-Konfiguration für duale Stromversorgung“ veranschaulicht.

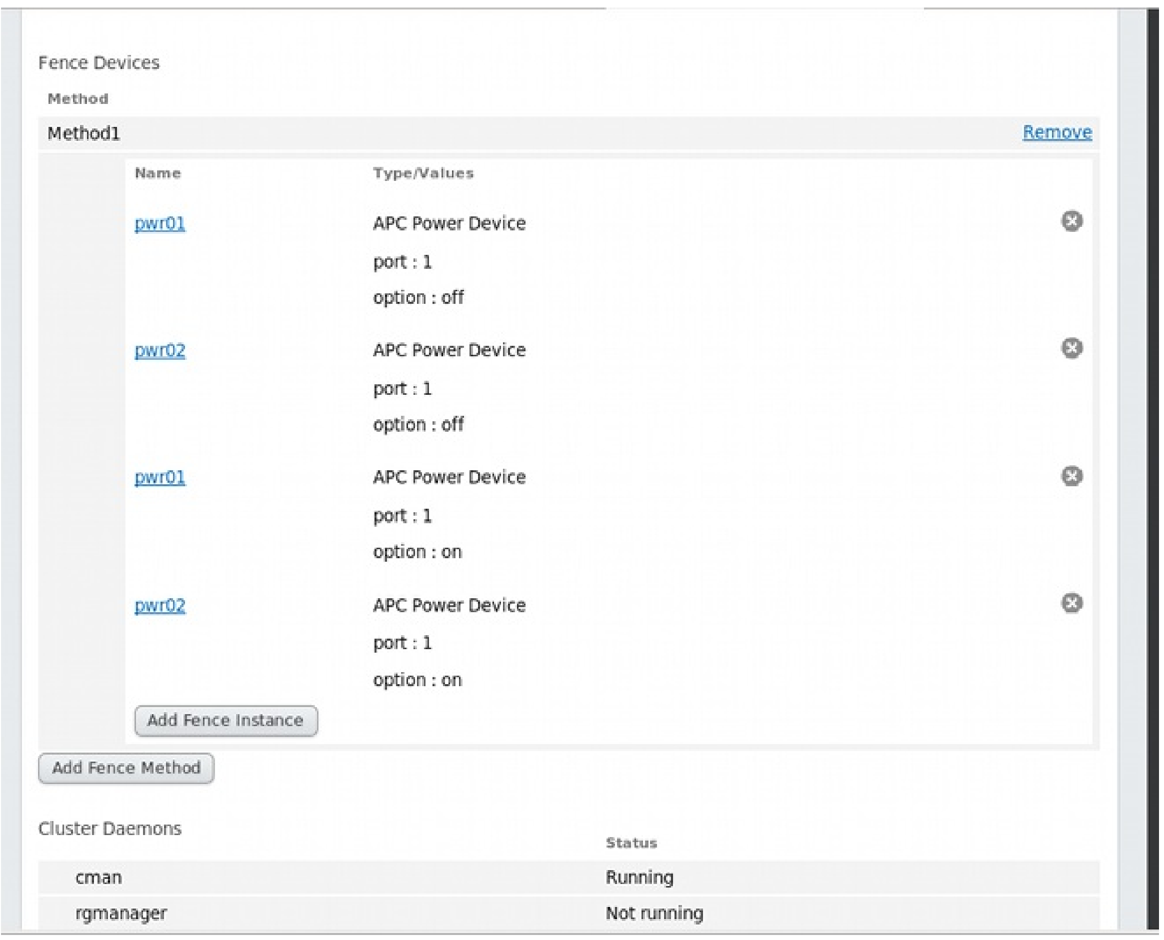


Abbildung 3.6. Fencing-Konfiguration für duale Stromversorgung

3.8. Konfiguration einer Ausfallsicherungs-Domain

Eine Ausfallsicherungs-Domain ist eine benannte Teilmenge von Cluster-Knoten, die dazu berechtigt ist, einen Cluster-Dienst im Falle eines Knotenausfalls weiterzuführen. Eine Ausfallsicherungs-Domain kann die folgenden Charakteristiken haben:

- Uneingeschränkt — Ermöglicht Ihnen, eine Teilmenge bevorzugter Mitglieder zu spezifizieren, doch der dieser Domain zugewiesene Cluster-Dienst kann auf jedem verfügbaren Mitglied ausgeführt werden.
- Eingeschränkt — Ermöglicht Ihnen, die Mitglieder einzuschränken, auf denen ein bestimmter Cluster-Dienst laufen darf. Falls keines der Mitglieder in einer eingeschränkten Ausfallsicherungs-Domain verfügbar ist, kann der Cluster-Dienst nicht gestartet werden (weder manuell noch durch die Cluster-Software).
- Ungeordnet — Wenn ein Cluster-Dienst einer ungeordneten Aufallsicherungs-Domain zugewiesen ist, wird das Mitglied, auf dem der Cluster-Dienst ausgeführt wird, ohne Berücksichtigung von Prioritäten aus den verfügbaren Mitgliedern der Ausfallsicherungs-Domain ausgewählt.
- Geordnet — Ermöglicht Ihnen, eine Prioritätsreihenfolge für die Mitglieder einer Ausfallsicherungs-Domain anzugeben. Das erste Mitglied in der Liste wird bevorzugt, gefolgt vom zweiten Mitglied in der Liste, usw.
- Failback — Ermöglicht Ihnen festzulegen, ob ein Dienst in der Ausfallsicherungs-Domain auf den Knoten zurückwechseln soll, auf dem er vor dessen Ausfall ursprünglich ausgeführt wurde. Das Konfigurieren dieser Charakteristik ist hilfreich in Situationen, in denen ein Knoten häufig ausfällt und Teil einer geordneten Ausfallsicherungs-Domain ist. In diesem Fall würde ein Dienst, der auf dem bevorzugten Knoten in einer Ausfallsicherungs-Domain läuft, möglicherweise wiederholt zwischen

dem bevorzugten Knoten und einem anderen Knoten hin- und her wechseln, was beträchtliche Leistungseinbußen zur Folge hätte.



Anmerkung

Die Failback-Charakteristik greift nur, wenn die geordnete Ausfallsicherung konfiguriert ist.



Anmerkung

Eine Änderung der Ausfallsicherungs-Domain-Konfiguration hat keine Auswirkungen auf derzeit laufende Dienste.



Anmerkung

Ausfallsicherungs-Domains werden für den Betrieb *nicht* benötigt.

Standardmäßig sind Ausfallsicherungs-Domains uneingeschränkt und ungeordnet.

In einem Cluster mit mehreren Mitgliedern kann Ihnen der Einsatz einer beschränkten Ausfallsicherungs-Domain die Arbeit erleichtern. Denn um einen Cluster zum Ausführen eines Cluster-Dienstes (wie z.B. **httpd**) einzurichten, müssen Sie auf allen Cluster-Mitgliedern, die diesen Cluster-Dienst ausführen sollen, eine identische Konfiguration einrichten. Anstatt den gesamten Cluster zur Ausführung dieses Cluster-Dienstes einzurichten, müssen Sie somit nur die Mitglieder der beschränkten Ausfallsicherungs-Domain, die Sie mit diesem Cluster-Dienst verknüpfen möchten, entsprechend einrichten.



Anmerkung

Um ein bevorzugtes Mitglied zu konfigurieren, können Sie eine uneingeschränkte Ausfallsicherungs-Domain einrichten, die nur aus einem Cluster-Mitglied besteht. Dadurch läuft der Cluster-Dienst zwar hauptsächlich auf diesem einen Cluster-Mitglied (dem bevorzugten Mitglied), doch erlaubt es dem Cluster-Dienst gleichzeitig, im Falle eines Ausfalls auf einen beliebigen anderen Knoten zu wechseln.

Die folgenden Abschnitte beschreiben das Hinzufügen, Ändern und Löschen einer Ausfallsicherungs-Domain:

- Abschnitt 3.8.1, „Hinzufügen einer Ausfallsicherungs-Domain“
- Abschnitt 3.8.2, „Ändern einer Ausfallsicherungs-Domain“
- Abschnitt 3.8.3, „Löschen einer Ausfallsicherungs-Domain“

3.8.1. Hinzufügen einer Ausfallsicherungs-Domain

Um eine Ausfallsicherungs-Domain hinzuzufügen, folgen Sie den Schritten in diesem Abschnitt.

1. Sie können auf der clusterspezifischen Seite Ausfallsicherungs-Domains für diesen Cluster konfigurieren, indem Sie auf **Failover Domains** (Ausfallsicherungs-Domains) oben in der Cluster-Ansicht klicken. Dadurch werden die Ausfallsicherungs-Domains angezeigt, die für diesen Cluster konfiguriert wurden.
2. Klicken Sie auf **Add** (Hinzufügen). Durch einen Klick auf **Add** wird das Dialogfeld **Add Failover Domain to Cluster** (Ausfallsicherungs-Domain zum Cluster hinzufügen) angezeigt, wie in Abbildung 3.7, „luci-Dialogfeld zur Konfiguration von Ausfallsicherungs-Domains“ veranschaulicht.

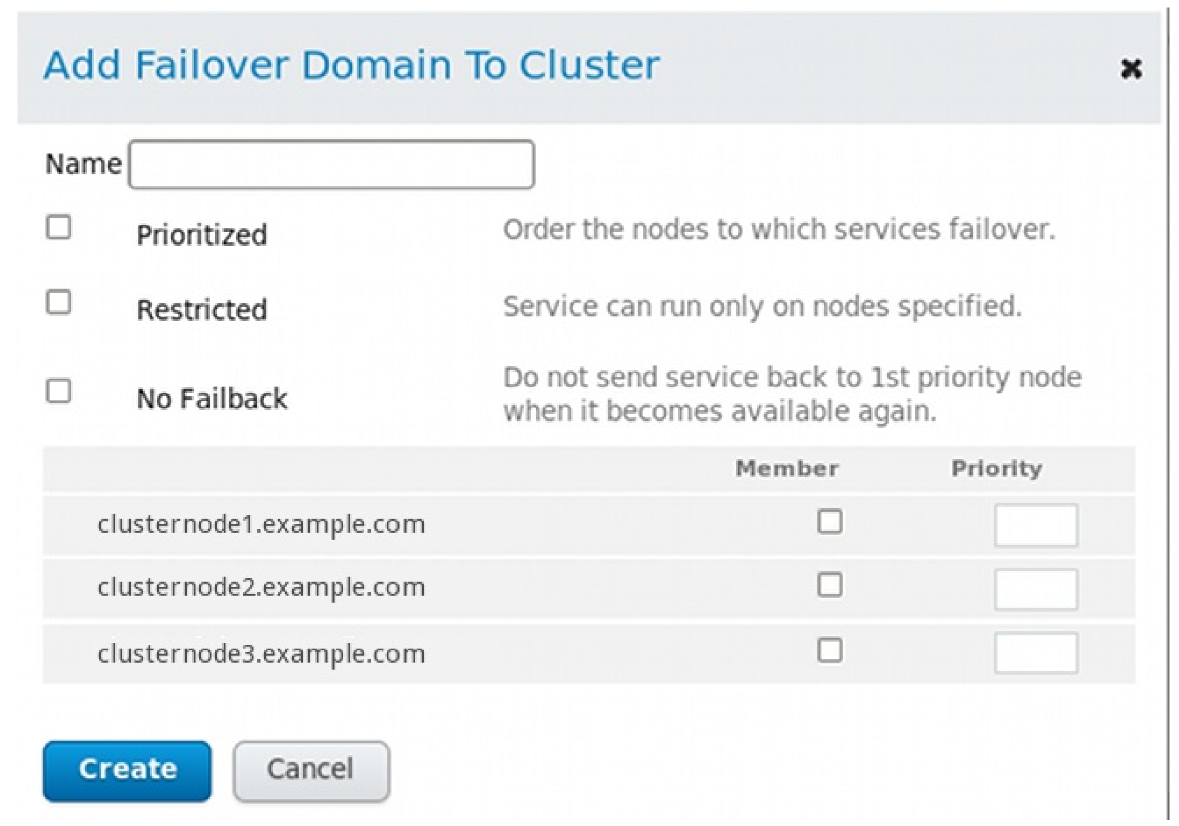
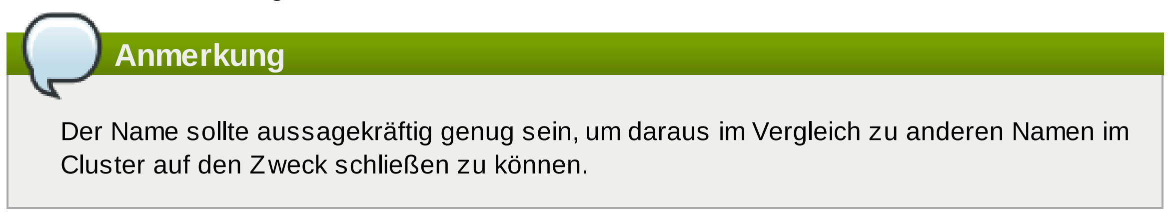


Abbildung 3.7. luci-Dialogfeld zur Konfiguration von Ausfallsicherungs-Domains

3. Geben Sie im Dialogfeld **`Add Failover Domain to Cluster`** im Textfeld **Name** einen Namen für die Ausfallsicherungs-Domain an.



Anmerkung

Der Name sollte aussagekräftig genug sein, um daraus im Vergleich zu anderen Namen im Cluster auf den Zweck schließen zu können.

4. Um das Erstellen von Ausfallsicherungsprioritäten für Mitglieder in einer Ausfallsicherungs-Domain zu aktivieren, markieren Sie das Auswahlkästchen **Prioritized** (Priorisiert). Ist **Prioritized** ausgewählt, können Sie den Prioritätswert **Priority** für jeden Knoten festlegen, der als Mitglied in der Ausfallsicherungs-Domain ausgewählt ist.
5. Um die Ausfallsicherung auf Mitglieder in dieser Ausfallsicherungs-Domain zu beschränken, markieren Sie das Auswahlkästchen **Restricted** (Eingeschränkt). Ist **Restricted** ausgewählt, werden Dienste, denen diese Ausfallsicherungs-Domain zugewiesen ist, im Fehlerfall nur auf Knoten innerhalb dieser Ausfallsicherungs-Domain wechseln.
6. Um festzulegen, dass ein Dienst in dieser Ausfallsicherungs-Domain nicht wieder auf den ursprünglichen Knoten zurückwechselt, markieren Sie das Auswahlkästchen **No Failback** (Kein Failback). Ist **No Failback** ausgewählt, so wird ein Dienst, der aufgrund eines Ausfalls von einem bevorzugten Knoten wechselt, nach dessen Wiederherstellung nicht wieder auf den ursprünglichen Knoten zurückwechseln.
7. Konfigurieren Sie Mitglieder für diese Ausfallsicherungs-Domain. Markieren Sie das Auswahlkästchen **Member** (Mitglied) für jeden Knoten, der Mitglied der Ausfallsicherungs-Domain sein soll. Falls **Prioritized** ausgewählt ist, stellen Sie im **Priority** Textfeld die Priorität für jedes Mitglied der Ausfallsicherungs-Domain ein.
8. Klicken Sie auf **`Create`** (Erstellen). Dadurch wird die Seite **`Failover Domains`** mit der neu erstellten Ausfallsicherungs-Domain angezeigt. Eine Meldung wird angezeigt, die besagt, dass die neue Domain erstellt wird. Aktualisieren Sie die Seite, um den aktuellen Status zu sehen.

3.8.2. Ändern einer Ausfallsicherungs-Domain

Um eine Ausfallsicherungs-Domain zu ändern, folgen Sie den Schritten in diesem Abschnitt.

1. Sie können auf der clusterspezifischen Seite Ausfallsicherungs-Domains für diesen Cluster konfigurieren, indem Sie auf **Failover Domains** (Ausfallsicherungs-Domains) oben in der Cluster-Ansicht klicken. Dadurch werden die Ausfallsicherungs-Domains angezeigt, die für diesen Cluster konfiguriert wurden.
2. Klicken Sie auf den Namen einer Ausfallsicherungs-Domain. Daraufhin wird die Konfigurationsseite für diese Ausfallsicherungs-Domain angezeigt.
3. Um die **Prioritized**, **Restricted** oder **No Failback** Eigenschaften für die Ausfallsicherungs-Domain zu ändern, setzen oder entfernen Sie das Häkchen im entsprechenden Auswahlkästchen für diese Eigenschaft und klicken Sie auf **`Update Properties`** (Eigenschaften aktualisieren).
4. Um die Mitgliedschaften der Ausfallsicherungs-Domain zu ändern, setzen oder entfernen Sie das Häkchen im Auswahlkästchen für die gewünschten Cluster-Mitglieder. Falls die Ausfallsicherungs-Domain priorisiert ist, können Sie auch die Prioritätseigenschaft für die Cluster-Mitglieder verändern. Klicken Sie zum Abschluss auf **`Update Settings`** (Einstellungen aktualisieren).

3.8.3. Löschen einer Ausfallsicherungs-Domain

Um eine Ausfallsicherungs-Domain zu löschen, folgen Sie den Schritten in diesem Abschnitt.

1. Sie können auf der clusterspezifischen Seite Ausfallsicherungs-Domains für diesen Cluster konfigurieren, indem Sie auf **Failover Domains** (Ausfallsicherungs-Domains) oben in der Cluster-Ansicht klicken. Dadurch werden die Ausfallsicherungs-Domains angezeigt, die für diesen Cluster konfiguriert wurden.
2. Markieren Sie das Auswahlkästchen der zu löschenden Ausfallsicherungs-Domain.
3. Klicken Sie auf **Delete** (Löschen).

3.9. Konfiguration von globalen Cluster-Eigenschaften

Sie können globale Ressourcen konfigurieren, die von jedem Dienst im Cluster verwendet werden dürfen, und Sie können Ressourcen konfigurieren, die nur einem bestimmten Dienst zur Verfügung stehen.

Um eine globale Cluster-Ressource hinzuzufügen, folgen Sie den Schritten in diesem Abschnitt. Sie können eine Ressource lokal für einen bestimmten Dienst hinzufügen, während Sie diesen Dienst konfigurieren, wie in Abschnitt 3.10, „Hinzufügen eines Cluster-Dienstes zum Cluster“ beschrieben.

1. Sie können auf der clusterspezifischen Seite Ressourcen für diesen Cluster hinzufügen, indem Sie auf **Resources** oben in der Cluster-Ansicht klicken. Dadurch werden die Ressourcen angezeigt, die für diesen Cluster konfiguriert wurden.
2. Klicken Sie auf **Add**. Dadurch erscheint das Drop-Down-Menü **Add Ressource to Cluster** (Ressource zum Cluster hinzufügen).
3. Klicken Sie auf das Drop-Down-Menü unter **Add Resource to Cluster** und wählen Sie den zu konfigurierenden Ressourcentyp.
4. Geben Sie die Ressourcenparameter für die hinzugefügte Ressource an. In Anhang B, *Parameter der Hochverfügbarkeitsressourcen* werden die Ressourcenparameter beschrieben.
5. Klicken Sie auf **`Submit`**. Durch den Klick auf **`Submit`** kehren Sie zur Ressourcenseite mit der **`Resources`** Anzeige zurück, auf der nun neben anderen Ressourcen auch die neu hinzugefügte Ressource angezeigt wird.

Um eine vorhandene Ressource zu ändern, führen Sie die folgenden Schritte aus.

1. Klicken Sie auf der **luci Resources** Seite auf den Namen der Ressource, die geändert werden soll. Daraufhin werden die Parameter für diese Ressource angezeigt.
2. Bearbeiten Sie die Ressourcenparameter.

3. Klicken Sie auf **Apply**.

Um eine vorhandene Ressource zu löschen, führen Sie die folgenden Schritte aus.

1. Markieren Sie auf der **luci Resources** Seite die Auswahlkästchen all jener Ressourcen, die Sie löschen möchten.
2. Klicken Sie auf **Delete**.

3.10. Hinzufügen eines Cluster-Dienstes zum Cluster

Um einen Cluster-Dienst zum Cluster hinzuzufügen, folgen Sie den Schritten in diesem Abschnitt.

1. Sie können auf der clusterspezifischen Seite Dienste für diesen Cluster hinzufügen, indem Sie auf **Service Groups** oben in der Cluster-Ansicht klicken. Dadurch werden die Dienste angezeigt, die für diesen Cluster konfiguriert wurden. (Auf der **Service Groups** Seite können Sie einen Dienst auch starten, stoppen und deaktivieren, wie in Abschnitt 4.5, „Verwaltung von Hochverfügbarkeitsdiensten“ beschrieben.)
2. Klicken Sie auf **Add**. Dadurch erscheint das Dialogfeld **Add Service Group to Cluster** (Dienstgruppe zu Cluster hinzufügen).
3. Geben Sie im Dialogfeld **Add Service Group to Cluster** den Namen des Dienstes im Textfeld **Service Name** ein.



Anmerkung

Der Name sollte aussagekräftig genug sein, um den Dienst klar von anderen Diensten im Cluster unterscheiden zu können.

4. Markieren Sie das Auswahlkästchen **Automatically Start This Service** (Diesen Dienst automatisch starten), falls Sie möchten, dass dieser Dienst beim Start des Clusters ebenfalls automatisch gestartet wird. Wird dieses Auswahlkästchen *nicht* markiert, muss der Dienst jedes Mal manuell gestartet werden, wenn der Cluster vom "Gestoppt"-Status wieder hochgefahren wird.
5. Markieren Sie das Auswahlkästchen **Run Exclusive** (Exklusiv ausführen), um die Richtlinie anzuwenden, nach der ein Dienst ausschließlich auf Knoten läuft, auf denen kein anderer Dienst ausgeführt wird.
6. Falls Sie Ausfallsicherungs-Domains für den Cluster konfiguriert haben, können Sie das Drop-Down-Menü des **Failover Domain** Parameters nutzen, um eine Ausfallsicherungs-Domain für diesen Dienst auszuwählen. Informationen über die Konfiguration von Ausfallsicherungs-Domains finden Sie in Abschnitt 3.8, „Konfiguration einer Ausfallsicherungs-Domain“.
7. Verwenden Sie die Drop-Down-Liste **Recovery Policy** (Richtlinie zur Wiederherstellung), um eine Richtlinie zur Wiederherstellung des Dienstes festzulegen. Mögliche Optionen für den Dienst sind **Relocate** (Verlegung), **Restart** (Neustart), **Restart-Disable** (Neustart-Deaktivierung) oder **Disable** (Deaktivierung).

   Wird die **Restart** Option ausgewählt, so versucht das System einen Neustart des ausgefallenen Dienstes, bevor der Dienst verlegt wird. Wird die **Relocate** Option ausgewählt, so versucht das System einen Neustart des Dienstes auf einem anderen Knoten. Wird die **Disable** Option gewählt, deaktiviert das System die Ressourcengruppe, falls eine der Komponenten ausfällt. Wird die **Restart-Disable** Option ausgewählt, versucht das System einen Neustart des ausgefallenen Dienstes an demselben Ort. Scheitert dieser Versuch, wird der Dienst deaktiviert, statt auf einen anderen Host im Cluster verlegt zu werden.

   Falls Sie **Restart** oder **Restart-Disable** als Wiederherstellungsrichtlinie für diesen Dienst auswählen, können Sie die maximale Anzahl an Neustart-Fehlschlägen festlegen, bevor der Dienst verlegt oder deaktiviert wird, sowie die Zeitspanne in Sekunden, nach der ein Neustart nicht weiter versucht werden soll.
8. Um eine Ressource zum Dienst hinzuzufügen, klicken Sie auf **Add Resource**. Durch den Klick

auf **Add Resource** wird das **Add Resource To Service** Drop-Down-Menü angezeigt, aus dem Sie eine vorhandene globale Ressource oder eine vorhandene lokale Ressource, die *nur* diesem Dienst zur Verfügung steht, hinzufügen können.



Anmerkung

Wenn Sie einen Cluster-Dienst konfigurieren, der eine IP-Adress-Ressource enthält, deren IP-Adresse geändert werden darf ("Floating"), müssen Sie die IP-Ressource als ersten Eintrag konfigurieren.

- Um eine vorhandene globale Ressource hinzuzufügen, klicken Sie im Drop-Down-Menü **Add Resource To Service** (Ressource zu Dienst hinzufügen) auf den Namen der vorhandenen Ressource. Daraufhin wird auf der **Service Groups** Seite für den Dienst, den Sie gerade konfigurieren, die Ressource und ihre Parameter angezeigt. Informationen über das Hinzufügen oder Verändern von globalen Ressourcen finden Sie in Abschnitt 3.9, „Konfiguration von globalen Cluster-Eigenschaften“).
- Um eine neue Ressource hinzuzufügen, die nur diesem Dienst zur Verfügung steht, wählen Sie den zu konfigurierenden Ressourcentyp aus dem Drop-Down-Menü **Add Resource To Service** und geben Sie die Ressourcenparameter für die hinzuzufügende Ressource an. In Anhang B, *Parameter der Hochverfügbarkeitsressourcen* werden die Ressourcenparameter beschrieben.
- Wenn Sie eine Ressource zu einem Dienst hinzufügen - egal, ob es sich dabei um eine vorhandene globale Ressource oder um eine nur für diesen Dienst verfügbare Ressource handelt - können Sie festlegen, ob diese Ressource ein **Independent Subtree** (Unabhängiger Unterbaum) oder eine **Non-Critical Resource** (Nicht-kritische Ressource) sein soll.

  Wenn Sie festlegen, dass eine Ressource ein unabhängiger Unterbaum sein soll, wird im Falle eines Ausfalls dieser Ressource nur diese Ressource neu gestartet (statt des gesamten Dienstes), bevor das System die normale Wiederherstellung versucht. Sie können die maximale Anzahl der zu versuchenden Neustarts für diese Ressource auf einem Knoten festlegen, bevor die Wiederherstellungsrichtlinie für diesen Dienst zur Anwendung kommt. Sie können auch eine Zeitspanne festlegen, nach der das System die Wiederherstellungsrichtlinie für den Dienst anwendet.

  Wenn Sie festlegen, dass die Ressource eine nicht-kritische Ressource ist, wird im Falle eines Ausfalls dieser Ressource nur diese Ressource neu gestartet, und falls die Ressource weiterhin fehlschlägt, wird nur diese Ressource deaktiviert (statt des gesamten Dienstes). Sie können die maximale Anzahl der zu versuchenden Neustarts für diese Ressource auf einem Knoten festlegen, bevor die Ressource deaktiviert wird. Sie können auch eine Zeitspanne festlegen, nach der das System die Ressource deaktiviert.

9. Falls Sie eine Kindressource zu der von Ihnen definierten Ressource hinzufügen möchten, klicken Sie auf **Add Child Resource** (Kindressource hinzufügen). Durch den Klick auf **Add Child Resource** wird das Drop-Down-Menü **Add Resource To Service** angezeigt, aus dem Sie eine vorhandene globale Ressource oder eine neue lokale Ressource, die nur diesem Dienst zur Verfügung steht, hinzufügen können. Je nach Bedarf können Sie weitere Kindressourcen zur Ihrer Ressource hinzufügen.



Anmerkung

Falls Sie eine Samba-Dienstressource hinzufügen, fügen Sie diese direkt zum Dienst hinzu, nicht als Kind einer anderen Ressource.



Anmerkung

Wenn Sie einen Abhängigkeitenbaum für einen Cluster-Dienst konfigurieren, der eine IP-Adress-Ressource enthält, deren IP-Adresse geändert werden darf ("Floating"), müssen Sie die IP-Ressource als ersten Eintrag konfigurieren und nicht als Kind einer anderen Ressource.

10. Wenn Sie damit fertig sind, Ressourcen zum Dienst und ggf. Kindressourcen zu den Ressourcen hinzuzufügen, klicken Sie auf **Submit**. Durch einen Klick auf **Submit** kehren Sie zur **Service Groups** Seite zurück, auf der neben den anderen Diensten nun auch der neu hinzugefügte Dienst angezeigt wird.



Anmerkung

Um die Existenz der in einem Cluster-Dienst verwendeten IP-Service-Ressourcen zu überprüfen, können Sie den **/sbin/ip addr show** Befehl auf einem Cluster-Knoten verwenden (anstelle des überholten **ifconfig** Befehls). Die folgende Ausgabe zeigt den **/sbin/ip addr show** Befehl auf einem Knoten ausgeführt auf dem ein Cluster-Dienst läuft:

```
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1356 qdisc pfifo_fast qlen 1000
    link/ether 00:05:5d:9a:d8:91 brd ff:ff:ff:ff:ff:ff
    inet 10.11.4.31/22 brd 10.11.7.255 scope global eth0
    inet6 fe80::205:5dff:fe9a:d891/64 scope link
    inet 10.11.4.240/22 scope global secondary eth0
       valid_lft forever preferred_lft forever
```

Um einen vorhandenen Dienst zu ändern, führen Sie die folgenden Schritte aus.

1. Klicken Sie im **Service Groups** Dialogfeld auf den Namen des Dienstes, der geändert werden soll. Daraufhin werden die Parameter und Ressourcen angezeigt, die für diesen Dienst konfiguriert wurden.
2. Bearbeiten Sie die Dienstparameter.
3. Klicken Sie auf **Submit**.

Um einen oder mehrere vorhandene Dienste zu löschen, führen Sie die folgenden Schritte aus.

1. Markieren Sie auf der **luci Service Groups** Seite die Auswahlkästchen all jener Dienste, die Sie löschen möchten.
2. Klicken Sie auf **Delete**.
3. Ab Red Hat Enterprise Linux 6.3 werden Sie von **luci** vor dem Löschen eines Dienstes in einer Warnmeldung dazu aufgefordert zu bestätigen, dass Sie die Dienstgruppen oder Gruppen wirklich löschen möchten, wodurch die darin enthaltenen Ressourcen gestoppt werden. Klicken Sie auf **Cancel**, um diesen Dialog zu schließen, ohne die Dienste zu löschen, oder klicken Sie auf **Proceed**, um mit dem Löschen der gewählten Dienste fortzufahren.

Kapitel 4. Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Conga

Dieses Kapitel erläutert die verschiedenen administrativen Aufgaben zur Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons und umfasst die folgenden Abschnitte:

- Abschnitt 4.1, „Hinzufügen eines vorhandenen Clusters zur luci-Oberfläche“
- Abschnitt 4.2, „Entfernen eines Clusters aus der luci-Oberfläche“
- Abschnitt 4.3, „Verwaltung von Cluster-Knoten“
- Abschnitt 4.4, „Starten, Stoppen, Neustarten und Löschen von Clustern“
- Abschnitt 4.5, „Verwaltung von Hochverfügbarkeitsdiensten“
- Abschnitt 4.6, „Sichern und Wiederherstellen der luci-Konfiguration“

4.1. Hinzufügen eines vorhandenen Clusters zur luci-Oberfläche

Wenn Sie bereits einen Hochverfügbarkeits-Add-On-Cluster erstellt hatten, können Sie diesen Cluster einfach zur **luci** Oberfläche hinzufügen, damit Sie diesen Cluster mit **Conga** verwalten können.

Um einen bereits vorhandenen Cluster zur **luci** Oberfläche hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf **Manage Clusters** (Cluster verwalten) aus dem Menü auf der linken Seite der **luci Homebase** Seite. Der Bildschirm **Clusters** erscheint.
2. Klicken Sie auf **Add** (Hinzufügen). Der Bildschirm **Add Existing Cluster** (Vorhandenen Cluster hinzufügen) erscheint.
3. Geben Sie den Knoten-Hostnamen und das **ricci** Passwort für einen beliebigen Knoten in dem vorhandenen Cluster an. Da jeder Knoten im Cluster sämtliche Konfigurationsinformationen des Clusters enthält, sollte dies genügend Informationen liefern, um den Cluster zur **luci** Oberfläche hinzuzufügen.
4. Klicken Sie auf **Connect** (Verbinden). Der Bildschirm **Add Existing Cluster** (Vorhandenen Cluster hinzufügen) zeigt daraufhin den Cluster-Namen und die verbleibenden Knoten im Cluster.
5. Geben Sie die jeweiligen **ricci** Passwörter für jeden Knoten im Cluster an, oder geben Sie nur ein Passwort an und wählen **Use same password for all nodes** (Dasselbe Passwort für alle Knoten im Cluster verwenden).
6. Klicken Sie auf **Add Cluster** (Cluster hinzufügen). Der bereits konfigurierte Cluster wird nun im Bildschirm **Manage Clusters** angezeigt.

4.2. Entfernen eines Clusters aus der luci-Oberfläche

Sie können einen Cluster aus der grafischen Verwaltungsoberfläche **luci** entfernen, ohne dass dies Auswirkungen auf die Cluster-Dienste oder die Cluster-Mitgliedschaft hat. Wenn Sie einen Cluster entfernen, können Sie diesen später wieder hinzufügen oder ihn einer anderen **luci** Instanz hinzufügen, wie in Abschnitt 4.1, „Hinzufügen eines vorhandenen Clusters zur luci-Oberfläche“ beschrieben.

Um einen Cluster von der grafischen Verwaltungsoberfläche **luci** zu entfernen, ohne die Cluster-Dienste oder die Cluster-Mitgliedschaft zu verändern, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf **Manage Clusters** (Cluster verwalten) aus dem Menü auf der linken Seite der **luci Homebase** Seite. Der Bildschirm **Clusters** erscheint.
2. Wählen Sie einen oder mehrere Cluster, die Sie entfernen möchten.
3. Klicken Sie auf **Remove**. Das System wird Sie dazu auffordern zu bestätigen, dass der Cluster aus der **luci** Verwaltungsoberfläche entfernt werden soll.

Für Informationen über das vollständige Löschen eines Clusters, das Stoppen aller Cluster-Dienste und das Löschen der Cluster-Konfigurationsdaten von den Knoten, siehe Abschnitt 4.4, „Starten, Stoppen,

Neustarten und Löschen von Clustern“.

4.3. Verwaltung von Cluster-Knoten

Dieser Abschnitt beschreibt, wie die folgenden Features zur Knotenverwaltung mithilfe der **luci** Server-Komponente von **Conga** durchgeführt werden:

- Abschnitt 4.3.1, „Einen Cluster-Knoten neu starten“
- Abschnitt 4.3.2, „Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen“
- Abschnitt 4.3.3, „Ein Mitglied zu einem laufenden Cluster hinzufügen“
- Abschnitt 4.3.4, „Ein Mitglied aus einem Cluster löschen“

4.3.1. Einen Cluster-Knoten neu starten

Um einen Knoten in einem Cluster neu zu starten, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** (Knoten) oben in der Cluster-Anzeige. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt. Dies ist zudem die Standardseite, die angezeigt wird, wenn Sie unter **Manage Clusters** im Menü auf der linken Seite der **luci Homebase** Seite auf den Cluster-Namen klicken.
2. Wählen Sie den neu zu startenden Knoten, indem Sie das Auswahlkästchen des gewünschten Knotens markieren.
3. Wählen Sie die **Reboot** (Neustart) Funktion aus dem Menü oben auf der Seite. Dies veranlasst den Knoten zu einem Neustart und es erscheint eine Meldung oben auf der Seite, die besagt, dass dieser Knoten derzeit neu gestartet wird.
4. Aktualisieren Sie die Seite, um den aktuellen Status des Knotens zu sehen.

Es ist auch möglich, mehrere Knoten gleichzeitig neu zu starten, indem Sie alle gewünschten Knoten auswählen und anschließend auf **Reboot** (Neustart) klicken.

4.3.2. Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen

Sie können die **luci** Server-Komponente von **Conga** dazu verwenden, um einen Knoten zum Verlassen eines aktiven Clusters zu veranlassen, indem Sie alle Cluster-Dienste auf diesem Knoten stoppen. Sie können die **luci** Server-Komponente von **Conga** auch dazu verwenden, um einen Knoten, der einen Cluster verlassen hat, wieder zum Eintreten in den Cluster zu veranlassen.

Wenn Sie einen Knoten zum Verlassen eines Clusters veranlassen, löscht dies nicht die Cluster-Konfigurationsinformationen auf diesem Knoten, und der Knoten erscheint nach wie vor in der Cluster-Knotenanzeige mit dem Vermerk **`Not a cluster member`** (Kein Cluster-Mitglied). Informationen über das vollständige Löschen eines Knotens aus der Cluster-Konfiguration finden Sie in Abschnitt 4.3.4, „Ein Mitglied aus einem Cluster löschen“.

Um einen Knoten zum Verlassen eines Clusters zu veranlassen, führen Sie die folgenden Schritte aus. Dadurch wird die Cluster-Software in dem Knoten beendet. Indem Sie einen Knoten dazu veranlassen, einen Cluster zu verlassen, wird verhindert, dass dieser Knoten automatisch wieder dem Cluster beitritt, wenn dieser neu startet.

1. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** (Knoten) oben in der Cluster-Anzeige. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt. Dies ist zudem die Standardseite, die angezeigt wird, wenn Sie unter **Manage Clusters** im Menü auf der linken Seite der **luci Homebase** Seite auf den Cluster-Namen klicken.
2. Wählen Sie den Knoten, der den Cluster verlassen soll, indem Sie das Auswahlkästchen für diesen Knoten markieren.
3. Wählen Sie die Funktion **Leave Cluster** (Cluster verlassen) aus dem Menü oben auf der Seite. Daraufhin erscheint eine Meldung oben auf der Seite, die besagt, dass dieser Knoten gestoppt wird.
4. Aktualisieren Sie die Seite, um den aktuellen Status des Knotens zu sehen.

Es ist auch möglich, mehrere Knoten gleichzeitig zum Verlassen des Clusters zu veranlassen, indem Sie alle gewünschten Knoten auswählen und anschließend auf **Leave Cluster** klicken.

Um einen Knoten zum Wiedereintritt in den Cluster zu veranlassen, wählen Sie alle Knoten, die dem Cluster wieder beitreten sollen, indem Sie deren Auswahlkästchen markieren und klicken Sie anschließend auf **Join Cluster** (Cluster beitreten). Dies veranlasst die ausgewählten Knoten dazu, dem Cluster wieder beizutreten, und es erlaubt den ausgewählten Knoten, dem Cluster automatisch beizutreten, wenn dieser neu gestartet wird.

4.3.3. Ein Mitglied zu einem laufenden Cluster hinzufügen

Um ein Mitglied zu einem laufenden Cluster hinzuzufügen, folgen Sie den Schritten in diesem Abschnitt.

1. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** oben in der Cluster-Anzeige. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt. Dies ist zudem die Standardseite, die angezeigt wird, wenn Sie unter **Manage Clusters** im Menü auf der linken Seite der **luci Homebase** Seite auf den Cluster-Namen klicken.
2. Klicken Sie auf **Add** (Hinzufügen). Durch einen Klick auf **Add** wird das Dialogfeld **`Add Nodes To Cluster`** (Knoten zu diesem Cluster hinzufügen) angezeigt.
3. Geben Sie in dem Textfeld **Node Hostname** den Knotennamen und im Textfeld **Password** das **ricci** Passwort ein. Falls Sie einen anderen Port für den **ricci** Agenten als den Standard 11111 verwenden, ändern Sie diesen Parameter auf den von Ihnen verwendeten Port.
4. Markieren Sie das Auswahlkästchen **Enable Shared Storage Support** (Unterstützung für gemeinsam verwendeten Speicher aktivieren), falls geclusterter Speicher erforderlich ist, um die Pakete herunterzuladen, die Unterstützung für geclusterten Speicher hinzufügen und um geclustertes LVM zu aktivieren. Sie sollten dies nur dann auswählen, wenn Sie Zugriff auf das Resilient Storage Add-On oder das Scalable File System Add-On haben.
5. Falls Sie weitere Knoten hinzufügen möchten, klicken Sie auf **`Add Another Node`** (Weiteren Knoten hinzufügen) und geben Sie den Knotennamen und das Passwort für jeden weiteren Knoten ein.
6. Klicken Sie auf **`Add Nodes`** (Knoten hinzufügen). Ein Klick auf **`Add Nodes`** löst die folgenden Aktionen aus:
   a. Falls Sie **Download Packages** (Pakete herunterladen) ausgewählt haben, werden die Cluster-Software-Pakete auf die Knoten heruntergeladen.
   b. Cluster-Software wird auf den Knoten installiert (bzw. es wird überprüft, ob die richtigen Software-Pakete installiert sind).
   c. Die Cluster-Konfigurationsdatei wird aktualisiert und an jeden Knoten im Cluster weitergereicht — einschließlich dem hinzugefügten Knoten.
   d. Der hinzugefügte Knoten tritt dem Cluster bei.

   Die Seite **Nodes** erscheint mit einer Meldung, die besagt, dass der Knoten derzeit zum Cluster hinzugefügt wird. Aktualisieren Sie die Seite, um den aktuellen Status zu sehen.
7. Sobald der Vorgang zum Hinzufügen eines Knotens abgeschlossen ist, klicken Sie auf den Knotennamen des neu hinzugefügten Knotens, um das Fencing für diesen Knoten wie in Abschnitt 3.6, „Konfiguration von Fencing-Geräten“ beschrieben zu konfigurieren.

4.3.4. Ein Mitglied aus einem Cluster löschen

Um ein Mitglied aus einem vorhandenen, derzeit laufenden Cluster zu löschen, folgen Sie den Schritten in diesem Abschnitt. Beachten Sie, dass vor dem Löschen von Knoten diese zunächst gestoppt werden müssen, es sei denn, Sie löschen alle Knoten im Cluster gleichzeitig.

1. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** oben in der Cluster-Anzeige. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt. Dies ist zudem die Standardseite, die angezeigt wird, wenn Sie unter **Manage Clusters** im Menü auf der linken Seite der **luci Homebase** Seite auf den Cluster-Namen klicken.



Anmerkung

Überspringen Sie den nächsten Schritt, um es Diensten zu ermöglichen, selbst auf einen anderen Knoten auszuweichen, wenn ihr Knoten gelöscht wird.

2. Deaktivieren oder Verlegen Sie jeden Dienst, der auf dem zu löschenden Knoten läuft. Informationen über das Deaktivieren oder Verlegen von Diensten finden Sie in Abschnitt 4.5, „Verwaltung von Hochverfügbarkeitsdiensten“.
3. Wählen Sie den bzw. die zu löschenden Knoten.
4. Klicken Sie auf **Delete** (Löschen). Die Seite **Nodes** zeigt an, dass der Knoten derzeit gelöscht wird. Aktualisieren Sie die Seite, um den aktuellen Status zu sehen.



Wichtig

Das Entfernen eines Cluster-Knotens von einem Cluster ist eine destruktive Operation, die nicht rückgängig gemacht werden kann.

4.4. Starten, Stoppen, Neustarten und Löschen von Clustern

Sie können einen Cluster starten, stoppen und neu starten, indem Sie diese Aktionen auf den einzelnen Knoten im Cluster ausführen. Klicken Sie auf der clusterspezifischen Seite auf **Nodes** oben in der Cluster-Anzeige. Dadurch werden die Knoten angezeigt, aus denen sich dieser Cluster zusammensetzt.

Die Start- und Neustartoperationen für Cluster-Knoten oder einen ganzen Cluster ermöglichen es Ihnen, die Cluster-Dienste vorübergehend zu unterbrechen, falls ein Cluster-Dienst beispielsweise auf ein anderes Cluster-Mitglied verlegt werden muss, da sein ursprünglicher Knoten gestoppt oder neu gestartet werden soll.

Um einen Cluster zu stoppen, führen Sie die folgenden Schritte aus. Dadurch wird die Cluster-Software in den Knoten beendet, allerdings verbleibt die Cluster-Konfigurationsinformationen auf diesen Knoten und sie erscheinen nach wie vor in der Cluster-Knotenanzeige mit dem Vermerk **Not a cluster member** (Kein Cluster-Mitglied).

1. Wählen Sie alle Knoten im Cluster, indem Sie das Auswahlkästchen neben jedem Knoten markieren.
2. Wählen Sie die Funktion **Leave Cluster** (Cluster verlassen) aus dem Menü oben auf der Seite. Daraufhin erscheint eine Meldung oben auf der Seite, die besagt, dass jeder Knoten gestoppt wird.
3. Aktualisieren Sie die Seite, um den aktuellen Status der Knoten zu sehen.

Um einen Cluster zu starten, führen Sie die folgenden Schritte aus:

1. Wählen Sie alle Knoten im Cluster, indem Sie das Auswahlkästchen neben jedem Knoten markieren.
2. Wählen Sie die Funktion **Join Cluster** (Cluster beitreten) aus dem Menü oben auf der Seite.
3. Aktualisieren Sie die Seite, um den aktuellen Status der Knoten zu sehen.

Um einen laufenden Cluster neu zu starten, stoppen Sie zunächst alle Knoten im Cluster an und starten anschließend wieder alle Knoten im Cluster, wie oben beschrieben.

Um einen Cluster vollständig zu löschen, führen Sie die folgenden Schritte aus. Dadurch werden alle Cluster-Dienste gestoppt, die Cluster-Konfigurationsdaten werden von den Knoten gelöscht und die Knoten aus der Cluster-Ansicht entfernt. Falls Sie später versuchen, einen vorhandenen Cluster hinzuzufügen unter Verwendung der Knoten, die Sie gelöscht haben, so wird **luci** darauf hinweisen,

dass der Knoten kein Mitglied eines Clusters ist.



Wichtig

Das Löschen eines Clusters ist eine destruktive Operation, die nicht wieder rückgängig gemacht werden kann. Um einen Cluster nach dessen Löschung wiederherzustellen, müssen Sie den Cluster von Grund auf neu erstellen und neu definieren.

1. Wählen Sie alle Knoten im Cluster, indem Sie das Auswahlkästchen neben jedem Knoten markieren.
2. Wählen Sie die Funktion **Delete** (Löschen) aus dem Menü oben auf der Seite.

Wenn Sie einen Cluster von der **luci** Oberfläche entfernen möchten, ohne einen der Cluster-Dienste zu stoppen oder eine Cluster-Mitgliedschaft zu ändern, können Sie die **Remove** Option auf der **Manage Clusters** Seite verwenden, wie in Abschnitt 4.2, „Entfernen eines Clusters aus der luci-Oberfläche“ beschrieben.

4.5. Verwaltung von Hochverfügbarkeitsdiensten

Zusätzlich zum Hinzufügen und Ändern eines Dienstes, wie in Abschnitt 3.10, „Hinzufügen eines Cluster-Dienstes zum Cluster“ beschrieben, können Sie die folgenden VerwaltungsFeatures für Hochverfügbarkeitsdienste über die **luci** Server-Komponente von **Conga** ausführen:

- Starten eines Dienstes
- Neustarten eines Dienstes
- Deaktivieren eines Dienstes
- Löschen eines Dienstes
- Verlegen eines Dienstes

Sie können auf der clusterspezifischen Seite Dienste für diesen Cluster verwalten, indem Sie auf **Service Groups** (Dienstgruppen) oben in der Cluster-Ansicht klicken. Dadurch werden die Dienste angezeigt, die für diesen Cluster konfiguriert wurden.

- **Starten eines Dienstes** — Um Dienste zu starten, die derzeit nicht ausgeführt werden, wählen Sie die gewünschten Dienste aus, indem Sie deren Auswahlkästchen markieren, und klicken Sie anschließend auf **Start**.
- **Neustart eines Dienstes** — Um Dienste neu zu starten, die derzeit ausgeführt werden, wählen Sie die gewünschten Dienste aus, indem Sie deren Auswahlkästchen markieren, und klicken Sie anschließend auf **Restart** (Neustart).
- **Deaktivieren eines Dienstes** — Um Dienste zu deaktivieren, die derzeit ausgeführt werden, wählen Sie die gewünschten Dienste aus, indem Sie deren Auswahlkästchen markieren, und klicken Sie anschließend auf **Disable** (Deaktivieren).
- **Löschen eines Dienstes** — Um Dienste zu löschen, die derzeit nicht ausgeführt werden, wählen Sie die gewünschten Dienste aus, indem Sie deren Auswahlkästchen markieren, und klicken Sie anschließend auf **Delete** (Löschen).
- **Verlegen eines Dienstes** — Um einen laufenden Dienst zu verlegen, klicken Sie in der Dienste-Seite auf den Namen des gewünschten Dienstes. Dadurch wird die Dienst-Konfigurationsseite für diesen Dienst angezeigt, der Sie unter anderem entnehmen können, auf welchem Knoten der Dienst derzeit läuft.

  Wählen Sie aus der Auswahlliste **`Start on node...`** (Starten auf Knoten...) denjenigen Knoten, auf den Sie diesen Dienst verlegen möchten, und klicken Sie anschließend auf das **Start** Symbol. Es erscheint eine Meldung oben auf der Seite, die besagt, dass dieser Knoten derzeit gestartet wird. Sie müssen ggf. die Seite neu laden, um schließlich die neue Meldung zu erhalten, dass der Dienst nun auf dem von Ihnen ausgewählten Knoten ausgeführt wird.



Anmerkung

Falls es sich bei dem laufenden Dienst, den Sie ausgewählt haben, um einen **vm** Dienst handelt, zeigt die Auswahlliste die **migrate** Option anstelle der **relocate** Option.



Anmerkung

Sie können auch einen einzelnen Dienst starten, neu starten oder löschen, indem Sie auf der **Services** Seite auf den Namen des Dienstes klicken. Dadurch wird die Dienst-Konfigurationsseite angezeigt. Oben rechts auf der Dienst-Konfigurationsseite sehen Sie dieselben Symbole für **Start**, **Restart**, **Disable** und **Delete**.

4.6. Sichern und Wiederherstellen der luci-Konfiguration

Ab der Red Hat Enterprise Linux 6.2 Release können Sie das folgende Verfahren nutzen, um eine Sicherungskopie der **luci** Datenbank zu erstellen, die in der **/var/lib/luci/data/luci.db** Datei gespeichert ist. Diese Datei ist nicht die Cluster-Konfiguration selbst (die in der **cluster.conf** Datei gespeichert ist), sondern sie enthält eine Liste mit Benutzern, Clustern und zugehörigen Eigenschaften, die von **luci** gepflegt werden. Standardmäßig wird die Sicherungskopie, die mithilfe dieses Verfahrens erstellt wird, in dasselbe Verzeichnis geschrieben, in der sich auch die **luci.db** Datei befindet.

1. Führen Sie den **service luci stop** Befehl durch.
2. Führen Sie den **service luci backup-db** Befehl durch.

   Optional können Sie einen Dateinamen als Parameter zum **backup-db** Befehl angeben, wodurch die **luci** Datenbank in die angegebene Datei geschrieben wird. Um die **luci** Datenbank beispielsweise in die Datei **/root/luci.db.backup** zu schreiben, können Sie den Befehl **service luci backup-db /root/luci.db.backup** ausführen. Beachten Sie, dass Sicherungsdateien, die an anderen Speicherorten als **/var/lib/luci/data/** abgelegt werden (Sicherungsdateien, deren Namen Sie zum Befehl **service luci backup-db** angeben), nicht in der Ausgabe des **list-backups** Befehls erscheinen.
3. Führen Sie **service luci start** aus.

Nutzen Sie das folgende Verfahren, um eine **luci** Datenbank wiederherzustellen.

1. Führen Sie den **service luci stop** Befehl durch.
2. Führen Sie **service luci list-backups** aus und notieren Sie sich den Namen der Datei, von der wiederhergestellt werden soll.
3. Führen Sie **service luci restore-db /var/lib/luci/data/*lucibackupfile*** aus, wobei ***lucibackupfile*** die Sicherungsdatei ist, von der wiederhergestellt werden soll.

   Der folgende Befehl stellt beispielsweise die **luci** Konfigurationsinformationen wieder her, die in der Sicherungsdatei **luci-backup20110923062526.db** gespeichert waren:

   ```
   service luci restore-db /var/lib/luci/data/luci-backup20110923062526.db
   ```
4. Führen Sie **service luci start** aus.

Angenommen, Sie müssen eine **luci** Datenbank wiederherstellen, haben jedoch aufgrund einer Neuinstallation die **host.pem** Datei auf dem Rechner verloren, auf dem Sie die Sicherung durchgeführt haben. In diesem Fall müssen Sie Ihre Cluster manuell wieder zu **luci** hinzufügen, um alle Cluster-Knoten erneut zu authentifizieren.

Nutzen Sie das folgende Verfahren, um eine **luci** Datenbank auf einem anderen Rechner

wiederherzustellen als dem, auf dem die Sicherung ursprünglich erstellt wurde. Beachten Sie, dass Sie neben der Datenbank selbst auch die SSL-Zertifikatsdatei kopieren müssen, damit sich **luci** bei den **ricci** Knoten authentifizieren kann. In diesem Beispiel wird die Sicherung auf dem Rechner **luci1** erstellt und auf dem Rechner **luci2** wiederhergestellt.

1. Führen Sie die folgende Befehlssequenz aus, um eine **luci** Sicherungsdatei auf **luci1** zu erstellen und um sowohl die SSL-Zertifikatsdatei als auch die **luci** Sicherungsdatei auf **luci2** zu kopieren.

```
[root@luci1 ~]# service luci stop
[root@luci1 ~]# service luci backup-db
[root@luci1 ~]# service luci list-backups
/var/lib/luci/data/luci-backup20120504134051.db
[root@luci1 ~]# scp /var/lib/luci/certs/host.pem /var/lib/luci/data/luci-
backup20120504134051.db root@luci2:
```

2. Stellen Sie sicher, dass auf dem **luci2** Rechner **luci** installiert wurde und derzeit nicht läuft. Installieren Sie das Paket, falls es noch nicht installiert wurde.
3. Führen Sie die folgende Befehlssequenz aus, um sicherzustellen, dass die Authentifizierung funktioniert, und um die **luci** Datenbank von **luci1** nach **luci2** zu kopieren.

```
[root@luci2 ~]# cp host.pem /var/lib/luci/certs/
[root@luci2 ~]# chown luci: /var/lib/luci/certs/host.pem
[root@luci2 ~]# /etc/init.d/luci restore-db ~/luci-
backup20120504134051.db
[root@luci2 ~]# shred -u ~/host.pem ~/luci-backup20120504134051.db
[root@luci2 ~]# service luci start
```

Kapitel 5. Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit dem ccs Befehl

Ab der Red Hat Enterprise Linux 6.1 Release bietet das Red Hat Hochverfügbarkeits-Add-On Unterstützung für den **ccs** Cluster-Konfigurationsbefehl. Der **ccs** Befehl ermöglicht es einem Administrator, die **cluster.conf** Cluster-Konfigurationsdatei zu erstellen, zu bearbeiten, oder anzusehen. Sie können den **ccs** Befehl verwenden, um eine Cluster-Konfigurationsdatei auf einem lokalen System oder auf einem entfernten Knoten zu konfigurieren. Mithilfe des **ccs** Befehls kann ein Administrator zudem die Cluster-Dienste auf einem oder allen Knoten in einem konfigurierten Cluster starten oder stoppen.

Dieses Kapitel beschreibt die Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software mithilfe des **ccs** Befehls. Informationen über die Verwendung des **ccs** Befehls zur Verwaltung eines laufenden Clusters finden Sie in Kapitel 6, *Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit **ccs***.

Dieses Kapitel umfasst die folgenden Abschnitte:

- Abschnitt 5.1, „Überblick über operationale Aspekte“
- Abschnitt 5.2, „Konfigurationsaufgaben“
- Abschnitt 5.3, „Starten von **ricci**“
- Abschnitt 5.4, „Erstellen eines Clusters“
- Abschnitt 5.5, „Konfigurieren von Fencing-Geräten“
- Abschnitt 5.7, „Konfigurieren von Fencing-Geräten für Cluster-Mitglieder“
- Abschnitt 5.8, „Konfigurieren einer Ausfallsicherungs-Domain“
- Abschnitt 5.9, „Konfigurieren von globalen Cluster-Ressourcen“
- Abschnitt 5.10, „Hinzufügen eines Cluster-Dienstes zum Cluster“
- Abschnitt 5.13, „Konfigurieren eines Quorumdatenträgers“
- Abschnitt 5.14, „Sonstige Cluster-Konfiguration“
- Abschnitt 5.14, „Sonstige Cluster-Konfiguration“
- Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“



Wichtig

Stellen Sie sicher, dass Ihre Bereitstellung des Red Hat Hochverfügbarkeits-Add-Ons Ihren Anforderungen gerecht wird und unterstützt werden kann. Beratschlagen Sie sich dazu ggf. mit einem autorisierten Red Hat Vertreter, um Ihre Konfiguration vor der Bereitstellung zu prüfen. Berücksichtigen Sie zudem eine gewisse Zeit für einen Burn-In-Test, um die Konfiguration auf mögliche Ausfälle zu überprüfen.



Wichtig

Dieses Kapitel verweist auf häufig verwendete **cluster.conf** Elemente und Parameter. Eine vollständige Liste samt Beschreibung aller **cluster.conf** Elemente und Parameter finden Sie im Cluster-Schema unter **/usr/share/cluster/cluster.rng** und das kommentierte Schema unter **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (zum Beispiel **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

5.1. Überblick über operationale Aspekte

Dieser Abschnitt beschreibt die folgenden, allgemeinen operationalen Aspekte des **ccs** Befehls zur Konfiguration eines Clusters:

- Abschnitt 5.1.1, „Erstellen der Cluster-Konfigurationsdatei auf einem lokalen System“
- Abschnitt 5.1.2, „Anzeigen der aktuellen Cluster-Konfiguration“
- Abschnitt 5.1.3, „Angeben des ricci-Passworts mit dem ccs-Befehl“
- Abschnitt 5.1.4, „Ändern von Cluster-Konfigurationskomponenten“

5.1.1. Erstellen der Cluster-Konfigurationsdatei auf einem lokalen System

Mithilfe des **ccs** Befehls können Sie eine Cluster-Konfigurationsdatei auf einem Cluster-Knoten erstellen, oder Sie können eine Cluster-Konfigurationsdatei auf einem lokalen Dateisystem erstellen und diese Datei anschließend auf einen Host in einem Cluster übertragen. Dies ermöglicht Ihnen, auf einem lokalen Rechner an der Datei zu arbeiten, diese unter Versionskontrolle zu verwalten, oder sie anderweitig je nach Bedarf zu kennzeichnen. Der **ccs** Befehl erfordert keine Root-Privilegien.

Wenn Sie mit dem **ccs** Befehl eine Cluster-Konfigurationsdatei auf einem Cluster-Knoten erstellen und bearbeiten, benutzen Sie die **-h** Option, um den Namen des Hosts anzugeben. Dieser Befehl erstellt und bearbeitet die **cluster.conf** Datei auf dem Host:

```
ccs -h host [options]
```

Um eine Cluster-Konfigurationsdatei auf einem lokalen System zu erstellen und zu bearbeiten, benutzen Sie die **-f** Option des **ccs** Befehls, um den Namen der Konfigurationsdatei anzugeben, wenn Sie eine Cluster-Operation ausführen. Sie können diese Datei nach Belieben benennen.

```
ccs -f file [options]
```

Nachdem Sie die Datei lokal erstellt haben, können Sie diese mithilfe der **--setconf** Option des **ccs** Befehls auf einen Cluster-Knoten übertragen. Auf einem Host-Rechner im Cluster wird die Datei **cluster.conf** benannt und im **/etc/cluster** Verzeichnis abgelegt.

```
ccs -h host -f file --setconf
```

Für weitere Informationen über die Verwendung der **--setconf** Option des **ccs** Befehls siehe Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“.

5.1.2. Anzeigen der aktuellen Cluster-Konfiguration

Wenn Sie zu irgendeinem Zeitpunkt während der Erstellung eines Cluster-Konfigurationsdatei die aktuelle Datei anzeigen möchten, verwenden Sie den folgenden Befehl unter Angabe eines Knotens im Cluster als Host:

```
ccs -h host --getconf
```

Falls Sie Ihre Cluster-Konfigurationsdatei auf einem lokalen System erstellen, können Sie die **-f** Option anstelle der **-h** Option angeben, wie in Abschnitt 5.1.1, „Erstellen der Cluster-Konfigurationsdatei auf einem lokalen System“ beschrieben.

5.1.3. Angeben des ricci-Passworts mit dem ccs-Befehl

Damit Sie den **ccs** Befehl dazu nutzen können, Kopien der **cluster.conf** Datei an die Knoten im Cluster zu verbreiten, ist es erforderlich, dass **ricci** auf den Cluster-Knoten installiert ist und läuft, wie in Abschnitt 2.13, „Überlegungen zu ricci“ beschrieben. Die Verwendung von **ricci** erfordert ein Passwort, wenn Sie zum ersten Mal von einem bestimmten Rechner aus mit **ricci** interagieren.

Falls Sie auf dem von Ihnen verwendeten Rechner noch kein Passwort für eine **ricci** Instanz auf einem bestimmten Rechner angegeben haben, werden Sie zur Eingabe dieses Passworts aufgefordert, wenn der **ccs** Befehl es benötigt. Alternativ können Sie die **-p** Option verwenden, um ein **ricci** Passwort auf der Befehlszeile anzugeben.

```
ccs -h host -p password --sync --activate
```

Wenn Sie die **cluster.conf** Datei mithilfe der **--sync** Option des **ccs** Befehls an alle Knoten im Cluster verbreiten und Sie dabei ein **ricci** Passwort im Befehl angeben, wird der **ccs** Befehl dieses Passwort für jeden Knoten im Cluster verwenden. Falls Sie auf den einzelnen Knoten jedoch verschiedene **ricci** Passwörter festlegen möchten, können Sie die **--setconf** Option mit der **-p** Option verwenden, um die Konfigurationsdatei nacheinander an alle Knoten einzeln zu verbreiten.

5.1.4. Ändern von Cluster-Konfigurationskomponenten

Verwenden Sie den **ccs** Befehl, um Cluster-Komponenten und Ihre Parameter in der Cluster-Konfigurationsdatei zu konfigurieren. Wenn Sie eine Cluster-Komponente zur Datei hinzugefügt haben und die Parameter dieser Komponente später verändern möchten, müssen Sie die definierte Komponente entfernen und sie mit den geänderten Parametern wieder hinzufügen. In den einzelnen Abschnitten dieses Kapitels finden Sie Informationen darüber, wie Sie dies für die jeweiligen Komponenten erreichen.

Die Parameter der **cman** Cluster-Komponente bieten eine Ausnahme von diesem Verfahren zur Modifizierung von Cluster-Komponenten. Um diese Parameter zu ändern, führen Sie die **--setcman** Option des **ccs** unter Angabe der neuen Parameter durch. Beachten Sie, dass durch die Angabe dieser Option alle Werte, die Sie nicht explizit festlegen, auf ihre Standardwerte zurückgesetzt werden, wie in Abschnitt 5.1.5, „Befehle, die vorhergehende Einstellungen überschreiben“ beschrieben.

5.1.5. Befehle, die vorhergehende Einstellungen überschreiben

Mehrere Optionen des **ccs** Befehls überschreiben beim Festlegen von Eigenschaften die vorherigen Einstellungen. Dies bedeutet, dass Sie den **ccs** Befehl mit einer dieser Optionen ohne Angabe von Einstellungen eingeben können und es werden alle Einstellungen auf die Standardwerte zurückgesetzt. Diese Optionen lauten:

- **--settotem**
- **--setdlm**
- **--setrm**
- **--setcman**
- **--setmulticast**
- **--setaltmulticast**
- **--setfencedaemon**
- **--setlogging**
- **--setquorumd**

Um beispielsweise alle Eigenschaften des Fencing-Deamons zurückzusetzen, können Sie den folgenden Befehl ausführen.

```
# ccs -h hostname --setfencedaemon
```

Beachten Sie jedoch, dass, wenn Sie einen dieser Befehle verwenden, um eine Eigenschaft neu einzustellen, die anderen Eigenschaften des Befehls wieder auf die Standardwerte zurückgesetzt werden. Zum Beispiel können Sie den folgenden Befehl verwenden, um die **post_fail_delay** Eigenschaft auf 5 zu setzen:

```
# ccs -h hostname --setfencedaemon post_fail_delay=5
```

Wenn Sie nach Ausführen dieses Befehls den folgenden Befehl ausführen, um die **post_join_delay** Eigenschaft auf 10 zurückzusetzen, wird die **post_fail_delay** Eigenschaft auf den Standardwert zurückgesetzt:

```
# ccs -h hostname --setfencedaemon post_join_delay=10
```

Um sowohl die **post_fail_delay** als auch die **post_join_delay** Eigenschaften neu einzustellen, geben Sie beide auf dem gleichen Befehl ein, wie im folgenden Beispiel:

```
# ccs -h hostname --setfencedaemon post_fail_delay=5 post_join_delay=10
```

Für mehr Information über die Konfiguration von Fencing-Geräten siehe Abschnitt 5.5, „Konfigurieren von Fencing-Geräten“.

5.1.6. Überprüfung der Konfiguration

Wenn Sie mit dem **ccs** Befehl die Cluster-Konfigurationsdatei erstellen und bearbeiten, wird die Konfiguration automatisch anhand des Cluster-Schemas auf ihre Gültigkeit überprüft. Ab der Red Hat Enterprise Linux 6.3 Release prüft der **ccs** Befehl die Konfiguration anhand des Cluster-Schemas unter **/usr/share/cluster/cluster.rng** auf demjenigen Knoten, den Sie mithilfe der **-h** Option spezifizieren. Bislang verwendete der **ccs** Befehl stets das Cluster-Schema, das im **ccs** Befehl integriert war, also **/usr/share/ccs/cluster.rng** auf dem lokalen System. Wenn Sie die **-f** Option verwenden, um das lokale System zu spezifizieren, so verwendet der **ccs** Befehl nach wie vor das Cluster-Schema **/usr/share/ccs/cluster.rng**, das im **ccs** Befehl enthalten war, auf dem lokalen System.

5.2. Konfigurationsaufgaben

Die Konfiguration der Red Hat Hochverfügbarkeits-Add-On Software mit **ccs** umfasst die folgenden Schritte:

1. Stellen Sie sicher, dass **ricci** auf allen Knoten im Cluster ausgeführt wird. Siehe Abschnitt 5.3, „Starten von ricci“.
2. Erstellen Sie einen Cluster. Siehe Abschnitt 5.4, „Erstellen eines Clusters“.
3. Konfigurieren Sie Fencing-Geräte. Siehe Abschnitt 5.5, „Konfigurieren von Fencing-Geräten“.
4. Konfigurieren Sie das Fencing für die Cluster-Mitglieder. Siehe Abschnitt 5.7, „Konfigurieren von Fencing-Geräten für Cluster-Mitglieder“.
5. Erstellen Sie Ausfallsicherungs-Domains. Siehe Abschnitt 5.8, „Konfigurieren einer Ausfallsicherungs-Domain“.
6. Erstellen Sie Ressourcen. Siehe Abschnitt 5.9, „Konfigurieren von globalen Cluster-Ressourcen“.
7. Erstellen Sie Cluster-Dienste. Siehe Abschnitt 5.10, „Hinzufügen eines Cluster-Dienstes zum Cluster“.
8. Konfigurieren Sie einen Quorumdatenträger, falls nötig. Siehe Abschnitt 5.13, „Konfigurieren eines Quorumdatenträgers“.
9. Konfigurieren Sie globale Cluster-Eigenschaften. Siehe Abschnitt 5.14, „Sonstige Cluster-Konfiguration“.
10. Verbreiten Sie die Cluster-Konfigurationsdatei auf allen Cluster-Knoten. Siehe Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“.

5.3. Starten von ricci

Um Cluster-Konfigurationsdateien zu erstellen und auf den Knoten im Cluster zu verbreiten, muss der **ricci** Dienst auf jedem Knoten laufen. Bevor Sie **ricci** starten, sollten Sie sich vergewissern, dass Sie Ihr System folgendermaßen konfiguriert haben:

1. Die IP-Ports auf Ihren Cluster-Knoten sind für **ricci** aktiviert. Für Informationen über das Aktivieren von IP-Ports auf Cluster-Knoten siehe Abschnitt 2.3.1, „Aktivieren von IP-Ports auf Cluster-Knoten“.
2. Der **ricci** Dienst ist auf allen Knoten im Cluster installiert, und es wurde ein **ricci** Passwort

zugewiesen, wie in Abschnitt 2.13, „Überlegungen zu **ricci**“ beschrieben.

Nachdem **ricci** auf jedem Knoten installiert und konfiguriert wurde, starten Sie den **ricci** Dienst auf jedem Knoten:

```
# service ricci start
Starting ricci:                                            [  OK  ]
```

5.4. Erstellen eines Clusters

Dieser Abschnitt beschreibt, wie Sie ein Gerüst für eine Cluster-Konfiguration ohne Fencing, Ausfallsicherungs-Domains und Hochverfügbarkeitsdiensten mithilfe des **ccs** Befehls erstellen, bearbeiten und löschen können. Nachfolgende Abschnitte beschreiben, wie diese Teile der Konfiguration erstellt werden.

Um ein Gerüst für eine Cluster-Konfigurationsdatei anzulegen, erstellen und benennen Sie zunächst den Cluster und fügen Sie anschließend Knoten zum Cluster hinzu, wie im folgenden Beispielverfahren veranschaulicht:

1. Erstellen Sie eine Cluster-Konfigurationsdatei auf einem der Knoten im Cluster, indem Sie den **ccs** Befehl mit dem **-h** Parameter ausführen, um den Knoten zu spezifizieren, auf dem die Datei erstellt werden soll, und die **createcluster** Option, um den Namen für den Cluster zu spezifizieren:

   ```
   ccs -h host --createcluster clustername
   ```

   Zum Beispiel erzeugt der folgende Befehl eine Konfigurationsdatei auf **node-01.example.com** namens **mycluster**:

   ```
   ccs -h node-01.example.com --createcluster mycluster
   ```

   Der Cluster-Name darf nicht länger als 15 Zeichen sein.

   Falls bereits eine **cluster.conf** Datei auf dem von Ihnen spezifizierten Host existiert, wird dieser Befehl die vorhandene Datei ersetzen.

   Wenn Sie eine Cluster-Konfigurationsdatei auf Ihrem lokalen System erstellen möchten, können Sie die **-f** Option anstelle der **-h** Option angeben. Für weitere Informationen zum lokalen Erstellen der Datei siehe Abschnitt 5.1.1, „Erstellen der Cluster-Konfigurationsdatei auf einem lokalen System“.

2. Um die Knoten zu konfigurieren, aus denen sich der Cluster zusammensetzt, führen Sie den folgenden Befehl für jeden Knoten im Cluster aus. Der Knotenname darf maximal 255 Bytes lang sein.

   ```
   ccs -h host --addnode node
   ```

   Beispielsweise fügen die folgenden drei Befehle die Knoten **node-01.example.com**, **node-02.example.com** und **node-03.example.com** zur Konfigurationsdatei auf **node-01.example.com** hinzu:

   ```
   ccs -h node-01.example.com --addnode node-01.example.com
   ccs -h node-01.example.com --addnode node-02.example.com
   ccs -h node-01.example.com --addnode node-03.example.com
   ```

   Um eine Liste der Knoten anzusehen, die für einen Cluster konfiguriert wurden, führen Sie den folgenden Befehl aus:

   ```
   ccs -h host --lsnodes
   ```

Beispiel 5.1, „**cluster.conf** Datei nach Hinzufügen von drei Knoten“ zeigt eine **cluster.conf** Konfigurationsdatei, nachdem Sie den Cluster **mycluster** erstellt haben, der die Knoten **node-01.example.com**, **node-02.example.com** und **node-03.example.com** enthält.

Beispiel 5.1. cluster.conf Datei nach Hinzufügen von drei Knoten

```
<cluster name="mycluster" config_version="2">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Wenn Sie einen Knoten zum Cluster hinzufügen, können Sie die Anzahl der Stimmen festlegen, über die der Knoten verfügt, und anhand derer bestimmt wird, ob ein Quorum vorliegt. Um die Anzahl der Stimmen für einen Cluster-Knoten zu spezifizieren, nutzen Sie folgenden Befehl:

```
ccs -h host --addnode host --votes votes
```

Wenn Sie einen Knoten hinzufügen, weist **ccs** dem Knoten einen eindeutigen, ganzzahligen Wert zu, der als Knotenkennung dient. Falls Sie die Knotenkennung bei der Erstellung des Knotens manuell festlegen möchten, verwenden Sie folgenden Befehl:

```
ccs -h host --addnode host --nodeid nodeid
```

Um einen Knoten aus dem Cluster zu entfernen, führen Sie den folgenden Befehl aus:

```
ccs -h host --rmnode node
```

Wenn Sie die Konfiguration aller Komponenten Ihres Clusters abgeschlossen haben, müssen Sie die Cluster-Konfigurationsdatei auf allen Knoten synchronisieren, wie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“ beschrieben.

5.5. Konfigurieren von Fencing-Geräten

Das Konfigurieren von Fencing-Geräten umfasst das Erstellen, Aktualisieren und Löschen von Fencing-Geräten für den Cluster. Sie müssen die Fencing-Geräte in einem Cluster erstellen und benennen, bevor Sie das Fencing für die Knoten im Cluster konfigurieren können. Werfen Sie für Informationen über das Konfigurieren von Fencing für die einzelnen Knoten im Cluster einen Blick auf Abschnitt 5.7, „Konfigurieren von Fencing-Geräten für Cluster-Mitglieder“.

Bevor Sie Ihre Fencing-Geräte konfigurieren, sollten Sie ggf. einige der Eigenschaften für den Fencing-Daemon für Ihr System abweichend von den Standardwerten erstellen. Die Werte, die Sie für den

Fencing-Daemon konfigurieren können, sind allgemeine Werte für den Cluster. Die allgemeinen Fencing-Eigenschaften für den Cluster, die Sie ggf. anpassen sollten, lassen sich wie folgt zusammenfassen:

- Der Parameter **post_fail_delay** (Verzögerung nach Ausfall) ist die Anzahl von Sekunden, die der Fencing-Daemon (**fenced**) wartet, bevor ein Knoten (ein Mitglied der Fencing-Domain) nach dessen Ausfall abgegrenzt wird. Der Standardwert für **post_fail_delay** ist **0**. Dieser Wert kann je nach Cluster- und Netzwerkleistung angepasst werden.
- Der Parameter **post-join_delay** (Verzögerung nach Beitritt) ist die Anzahl der Sekunden, die der Fencing-Daemon (**fenced**) wartet, bevor ein Knoten abgegrenzt wird nachdem der Knoten der Fencing-Domain beitritt. Der **post-join_delay** Standardwert ist **6**. Eine typische Einstellung für **post-join_delay** liegt zwischen 20 und 30 Sekunden, kann aber je nach Cluster- und Netzwerkleistung variieren.

Sie setzen die Werte der **post_fail_delay** und **post_join_delay** Parameter mit der **--setfencedaemon** Option des **ccs** Befehls. Beachten Sie jedoch, dass die Ausführung des **ccs --setfencedaemon** Befehls alle vorhandenen Fencing-Daemon-Eigenschaften, die explizit gesetzt wurden, überschreibt und sie auf die Standardwerte zurücksetzt.

Um beispielsweise einen Wert für den **post_fail_delay** Parameter zu konfigurieren, führen Sie den folgenden Befehl aus. Dieser Befehl überschreibt die Werte aller anderen bestehenden Fencing-Daemon-Eigenschaften, die Sie mit diesem Befehl gesetzt haben und stellt sie auf die Standardwerte zurück.

```
ccs -h host --setfencedaemon post_fail_delay=value
```

Um einen Wert für den **post_join_delay** Parameter zu konfigurieren, führen Sie den folgenden Befehl aus. Dieser Befehl überschreibt die Werte aller anderen bestehenden Fencing-Daemon-Eigenschaften, die Sie mit diesem Befehl gesetzt haben und stellt sie auf die Standardwerte zurück.

```
ccs -h host --setfencedaemon post_join_delay=value
```

Um einen Wert sowohl für den **post_join_delay** Parameter als auch den **post_fail_delay** Parameter zu konfigurieren, führen Sie den folgenden Befehl aus:

```
ccs -h host --setfencedaemon post_fail_delay=value post_join_delay=value
```



Anmerkung

Weitere Informationen über die **post_join_delay** und **post_fail_delay** Parameter sowie weitere, konfigurierbare Fencing-Daemon-Eigenschaften finden Sie auf der fenced(8) Handbuchseite. Werfen Sie auch einen Blick auf das Cluster-Schema unter **/usr/share/cluster/cluster.rng** und das kommentierte Schema unter **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html**.

Um ein Fencing-Gerät für einen Cluster zu konfigurieren, führen Sie den folgenden Befehl aus:

```
ccs -h host --addfencedev devicename [fencedeviceoptions]
```

Um beispielsweise in der Konfigurationsdatei auf dem Cluster-Knoten **node1** ein APC-Fencing-Gerät namens **my_apc** mit der IP-Adresse **apc_ip_example**, mit dem Login **login_example** und dem Passwort **password_example** zu erstellen, führen Sie den folgenden Befehl aus:

```
ccs -h node1 --addfencedev myfence agent=fence_apc ipaddr=apc_ip_example
login=login_example passwd=password_example
```

Das folgende Beispiel zeigt den **fencedevices** Abschnitt der **cluster.conf** Konfigurationsdatei, nachdem Sie dieses APC-Fencing-Gerät hinzugefügt haben:

```
<fencedevices>
      <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="my_apc" passwd="password_example"/>
</fencedevices>
```

Bei der Konfiguration von Fencing-Geräten für einen Cluster kann es hilfreich sein, eine Liste der Geräte zu sehen, die für Ihren Cluster zur Verfügung stehen, sowie die jeweiligen Optionen, die für diese Geräte verfügbar sind. Auch kann es hilfreich sein, eine Liste aller derzeit für Ihren Cluster konfigurierten Fencing-Geräte zu sehen. Für mehr Informationen über die Verwendung von **ccs**, um eine Liste verfügbarer Fencing-Geräte und Optionen bzw. eine Liste derzeit konfigurierter Fencing-Geräte für Ihren Cluster anzuzeigen, werfen Sie einen Blick auf Abschnitt 5.6, „Auflisten von Fencing-Geräten und Fencing-Geräteoptionen“.

Um ein Fencing-Gerät aus Ihrer Cluster-Konfiguration zu entfernen, führen Sie den folgenden Befehl aus:

```
ccs -h host --rmfencedev fence_device_name
```

Um beispielsweise ein Fencing-Gerät namens **myfence** aus der Cluster-Konfigurationsdatei auf dem Cluster-Knoten **node1** zu löschen, führen Sie den folgenden Befehl aus:

```
ccs -h node1 --rmfencedev myfence
```

Falls Sie die Parameter eines bereits konfigurierten Fencing-Geräts nachträglich ändern möchten, müssen Sie dieses Fencing-Gerät entfernen und mit den geänderten Parametern anschließend wieder hinzufügen.

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“ beschrieben.

5.6. Auflisten von Fencing-Geräten und Fencing-Geräteoptionen

Sie können den **ccs** Befehl verwenden, um eine Liste aller verfügbaren Fencing-Geräte anzuzeigen und um eine Liste mit Optionen für die jeweiligen Fencing-Typen anzuzeigen. Auch können Sie mit dem **ccs** Befehl eine Liste aller Fencing-Geräte anzeigen, die derzeit für Ihren Cluster konfiguriert sind.

Um eine Liste aller derzeit für Ihren Cluster verfügbaren Fencing-Geräte auszugeben, führen Sie den folgenden Befehl aus:

```
ccs -h host --lsfenceopts
```

Beispielsweise zeigt der folgende Befehl die Fencing-Geräte, die auf dem Cluster-Knoten **node1** verfügbar sind.

```
[root@ask-03 ~]# ccs -h node1 --lsfenceopts
fence_rps10 - RPS10 Serial Switch
fence_vixel - No description available
fence_egenera - No description available
fence_xcat - No description available
fence_na - Node Assassin
fence_apc - Fence agent for APC over telnet/ssh
fence_apc_snmp - Fence agent for APC over SNMP
fence_bladecenter - Fence agent for IBM BladeCenter
fence_bladecenter_snmp - Fence agent for IBM BladeCenter over SNMP
fence_cisco_mds - Fence agent for Cisco MDS
fence_cisco_ucs - Fence agent for Cisco UCS
fence_drac5 - Fence agent for Dell DRAC CMC/5
fence_eps - Fence agent for ePowerSwitch
fence_ibmblade - Fence agent for IBM BladeCenter over SNMP
fence_ifmib - Fence agent for IF MIB
fence_ilo - Fence agent for HP iLO
fence_ilo_mp - Fence agent for HP iLO MP
fence_intelmodular - Fence agent for Intel Modular
fence_ipmilan - Fence agent for IPMI over LAN
fence_kdump - Fence agent for use with kdump
fence_rhevm - Fence agent for RHEV-M REST API
fence_rsa - Fence agent for IBM RSA
fence_sanbox2 - Fence agent for QLogic SANBox2 FC switches
fence_scsi - fence agent for SCSI-3 persistent reservations
fence_virsh - Fence agent for virsh
fence_virt - Fence agent for virtual machines
fence_vmware - Fence agent for VMware
fence_vmware_soap - Fence agent for VMware over SOAP API
fence_wti - Fence agent for WTI
fence_xvm - Fence agent for virtual machines
```

Führen Sie den folgenden Befehl aus, um eine Liste aller Optionen anzuzeigen, die Sie für einen bestimmten Fencing-Typ spezifizieren können:

```
ccs -h host --lsfenceopts fence_type
```

Beispielsweise zeigt der folgende Befehl die Fencing-Optionen, die für den Fencing-Agenten **fence_wti** verfügbar sind.

```
[root@ask-03 ~]# ccs -h node1 --lsfenceopts fence_wti
fence_wti - Fence agent for WTI
  Required Options:
  Optional Options:
    option: No description available
    action: Fencing Action
    ipaddr: IP Address or Hostname
    login: Login Name
    passwd: Login password or passphrase
    passwd_script: Script to retrieve password
    cmd_prompt: Force command prompt
    secure: SSH connection
    identity_file: Identity file for ssh
    port: Physical plug number or name of virtual machine
    inet4_only: Forces agent to use IPv4 addresses only
    inet6_only: Forces agent to use IPv6 addresses only
    ipport: TCP port to use for connection with device
    verbose: Verbose mode
    debug: Write debug information to given file
    version: Display version information and exit
    help: Display help and exit
    separator: Separator for CSV created by operation list
    power_timeout: Test X seconds for status change after ON/OFF
    shell_timeout: Wait X seconds for cmd prompt after issuing command
    login_timeout: Wait X seconds for cmd prompt after login
    power_wait: Wait X seconds after issuing ON/OFF
    delay: Wait X seconds before fencing is started
    retry_on: Count of attempts to retry power on
```

Um eine Liste aller derzeit für Ihren Cluster konfigurierten Fencing-Geräte auszugeben, führen Sie den folgenden Befehl aus:

```
ccs -h host --lsfencedev
```

5.7. Konfigurieren von Fencing-Geräten für Cluster-Mitglieder

Nachdem Sie die ersten Schritte zum Erstellen eines Clusters und zum Erstellen von Fencing-Geräten abgeschlossen haben, müssen Sie nun das Fencing für die Cluster-Knoten konfigurieren. Um das Fencing für die Knoten zu konfigurieren, folgen Sie den Schritten in diesem Abschnitt. Beachten Sie, dass Sie das Fencing für jeden Knoten im Cluster konfigurieren müssen.



Anmerkung

Es wird empfohlen, für jeden Knoten mehrere Fencing-Mechanismen zu konfigurieren. Ein Fencing-Gerät kann aus verschiedenen Gründen ausfallen, beispielsweise aufgrund einer Netzwerkspaltung, eines Stromausfalls oder eines Problems mit dem Fencing-Gerät selbst. Die Konfiguration mehrerer Fencing-Mechanismen verringert die Wahrscheinlichkeit, dass der Ausfall eines Fencing-Geräts schwerwiegende Folgen hat.

Dieser Abschnitt dokumentiert die folgenden Verfahren:

- Abschnitt 5.7.1, „Konfiguration eines einzelnen Power-Fencing-Geräts für einen Knoten“
- Abschnitt 5.7.2, „Konfiguration eines einzelnen Speicher-Fencing-Geräts für einen Knoten“
- Abschnitt 5.7.3, „Konfiguration eines Backup-Fencing-Geräts“
- Abschnitt 5.7.4, „Konfiguration eines Knotens mit redundanter Stromversorgung“
- Abschnitt 5.7.5, „Entfernen von Fencing-Methoden und Fencing-Instanzen“

5.7.1. Konfiguration eines einzelnen Power-Fencing-Geräts für einen Knoten

Verwenden Sie folgendes Verfahren, um einen Knoten mit einem einzelnen Power-Fencing-Gerät zu konfigurieren, welches das Fencing-Gerät namens **my_apc** verwendet, welches wiederum den **fence_apc** Fencing-Agenten verwendet. In diesem Beispiel wurde das Gerät namens **my_apc** bereits mit der **--addfencedev** Option konfiguriert, wie in Abschnitt 5.5, „Konfigurieren von Fencing-Geräten" beschrieben.

1. Fügen Sie eine Fencing-Methode für den Knoten hinzu und geben Sie einen Namen für die Fencing-Methode an.

   ```
   ccs -h host --addmethod method node
   ```

   Um beispielsweise eine Fencing-Methode namens **APC** für den Knoten **node-01.example.com** in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, führen Sie den folgenden Befehl aus:

   ```
   ccs -h node01.example.com --addmethod APC node01.example.com
   ```

2. Fügen Sie eine Fencing-Instanz für die Methode hinzu. Sie müssen angeben, welches Fencing-Gerät für den Knoten verwendet werden soll, den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, sowie jegliche Optionen für diese Methode speziell für diesen Knoten:

   ```
   ccs -h host --addfenceinst fencedevicename node method [options]
   ```

   Um beispielsweise eine Fencing-Instanz in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, die den APC Switch Power-Port 1 auf dem Fencing-Gerät namens **my_apc** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung der Methode namens **APC** abzugrenzen, verwenden Sie folgenden Befehl:

   ```
   ccs -h node01.example.com --addfenceinst my_apc node01.example.com APC
   port=1
   ```

Sie müssen für jeden Knoten im Cluster eine Fencing-Methode hinzufügen. Die folgenden Befehle konfigurieren eine Fencing-Methode für jeden Knoten mit dem Methodennamen **APC**. Das Gerät für die Fencing-Methode spezifiziert **my_apc** als Gerätename, wobei es sich hierbei um ein Gerät handelt, das bereits vorher mit der **--addfencedev** Option konfiguriert wurde, wie in Abschnitt 5.5, „Konfigurieren von Fencing-Geräten" beschrieben. Jeder Knoten ist mit einer eindeutigen APC Switch Power-Port-Nummer konfiguriert: Die Port-Nummer für **node-01.example.com** ist **1**, die Port-Nummer für **node-02.example.com** ist **2**, und die Port-Nummer für **node-03.example.com** ist **3**.

```
ccs -h node01.example.com --addmethod APC node01.example.com
ccs -h node01.example.com --addmethod APC node02.example.com
ccs -h node01.example.com --addmethod APC node03.example.com
ccs -h node01.example.com --addfenceinst my_apc node01.example.com APC port=1
ccs -h node01.example.com --addfenceinst my_apc node02.example.com APC port=2
ccs -h node01.example.com --addfenceinst my_apc node03.example.com APC port=3
```

Beispiel 5.2, „**cluster.conf** nach Hinzufügen von Power-Fencing-Methoden" zeigt eine **cluster.conf** Konfigurationsdatei, nachdem Sie diese Fencing-Methoden und Instanzen zu jedem Knoten im Cluster hinzugefügt haben.

Beispiel 5.2. `cluster.conf` nach Hinzufügen von Power-Fencing-Methoden

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="my_apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="my_apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="my_apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="my_apc" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“ beschrieben.

5.7.2. Konfiguration eines einzelnen Speicher-Fencing-Geräts für einen Knoten

Für andere Fencing-Methoden als das Power-Fencing (also SAN/Speicher-Fencing) müssen Sie *Unfencing* für das Fencing-Gerät konfigurieren. Dadurch wird sichergestellt, dass ein abgegrenzter Knoten erst wieder re-aktiviert wird, nachdem er neu gestartet wurde. Wenn Sie ein Gerät konfigurieren, dass Unfencing erfordert, muss der Cluster zunächst gestoppt werden, dann muss die vollständige Konfiguration einschließlich Geräte und Unfencing hinzugefügt werden, bevor der Cluster gestartet wird.

Wenn Sie Unfencing für einen Knoten konfigurieren, spezifizieren Sie ein Gerät als Spiegelbild des jeweiligen Fencing-Geräts für den Knoten, mit dem Unterschied, dass es die explizite Aktion **`on`** oder **`enable`** enthält.

Für weitere Informationen über das Unfencing von Knoten werfen Sie einen Blick auf die **`fence_node`**(8) Handbuchseite.

Verwenden Sie das folgende Verfahren, um einen Knoten mit einem einzelnen Speicher-Fencing-Gerät zu konfigurieren, das ein Fencing-Gerät namens **`sanswitch1`** verwendet, welches wiederum den **`fence_sanbox2`** Fencing-Agenten verwendet.

1. Fügen Sie eine Fencing-Methode für den Knoten hinzu und geben Sie einen Namen für die Fencing-Methode an.

```
ccs -h host --addmethod method node
```

Um beispielsweise eine Fencing-Methode namens **SAN** für den Knoten **node-01.example.com** in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, führen Sie den folgenden Befehl aus:

```
ccs -h node01.example.com --addmethod SAN  node01.example.com
```

2. Fügen Sie eine Fencing-Instanz für die Methode hinzu. Sie müssen angeben, welches Fencing-Gerät für den Knoten verwendet werden soll, den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, sowie jegliche Optionen für diese Methode speziell für diesen Knoten:

```
ccs -h host --addfenceinst fencedevicename node method [options]
```

Um beispielsweise eine Fencing-Instanz in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, die den SAN Switch Power-Port 11 auf dem Fencing-Gerät namens **sanswitch1** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung der Methode namens **SAN** abzugrenzen, verwenden Sie folgenden Befehl:

```
ccs -h node01.example.com --addfenceinst sanswitch1 node01.example.com SAN
port=11
```

3. Um Unfencing für das Speicher-Fencing-Gerät auf diesem Knoten zu konfigurieren, führen Sie den folgenden Befehl aus:

```
ccs -h host --addunfence fencedevicename node action=on|off
```

Sie müssen für jeden Knoten im Cluster eine Fencing-Methode hinzufügen. Die folgenden Befehle konfigurieren eine Fencing-Methode für jeden Knoten mit dem Methodennamen **SAN**. Das Gerät für die Fencing-Methode spezifiziert **sanswitch** als Gerätename, wobei es sich hierbei um ein Gerät handelt, die bereits vorher mit der --addfencedev Option konfiguriert wurde, wie in Abschnitt 5.5, „Konfigurieren von Fencing-Geräten“ beschrieben. Jeder Knoten ist mit einer eindeutigen SAN physischen Port-Nummer konfiguriert: Die Port-Nummer für **node-01.example.com** ist **11**, die Port-Nummer für **node-02.example.com** ist **12**, und die Port-Nummer für **node-03.example.com** ist **13**.

```
ccs -h node01.example.com --addmethod SAN node01.example.com
ccs -h node01.example.com --addmethod SAN node02.example.com
ccs -h node01.example.com --addmethod SAN node03.example.com
ccs -h node01.example.com --addfenceinst sanswitch1 node01.example.com SAN port=11
ccs -h node01.example.com --addfenceinst sanswitch1 node02.example.com SAN port=12
ccs -h node01.example.com --addfenceinst sanswitch1 node03.example.com SAN port=13
ccs -h node01.example.com --addunfence sanswitch1 node01.example.com port=11
action=on
ccs -h node01.example.com --addunfence sanswitch1 node02.example.com port=12
action=on
ccs -h node01.example.com --addunfence sanswitch1 node03.example.com port=13
action=on
```

Beispiel 5.3, „**cluster.conf** nach Hinzufügen von Speicher-Fencing-Methoden“ zeigt eine **cluster.conf** Konfigurationsdatei, nachdem Sie Fencing-Methoden, Fencing-Instanzen und Unfencing für jeden Knoten im Cluster hinzugefügt haben:

Beispiel 5.3. `cluster.conf` nach Hinzufügen von Speicher-Fencing-Methoden

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="SAN">
       <device name="sanswitch1" port="11"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="11" action="on"/>
         </unfence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="SAN">
       <device name="sanswitch1" port="12"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="12" action="on"/>
         </unfence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="SAN">
       <device name="sanswitch1" port="13"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="13" action="on"/>
         </unfence>
     </clusternode>
   </clusternodes>
   <fencedevices>
        <fencedevice agent="fence_sanbox2" ipaddr="san_ip_example"
login="login_example" name="sanswitch1" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“ beschrieben.

5.7.3. Konfiguration eines Backup-Fencing-Geräts

Sie können mehrere Fencing-Methoden für einen Knoten definieren. Falls die Abgrenzung mit der ersten Methode fehlschlägt, wird das System versuchen, den Knoten mithilfe der zweiten Methode abzugrenzen, gefolgt von jeglichen zusätzlichen konfigurierten Methoden. Um eine Backup-Fencing-Methode für einen Knoten zu konfigurieren, konfigurieren Sie zwei Methoden für einen Knoten und eine Fencing-Instanz für jede Methode.



Anmerkung

Die Reihenfolge, in der das System die konfigurierten Fencing-Methoden einsetzt, entspricht ihrer Reihenfolge in der Cluster-Konfigurationsdatei. Die erste Methode, die Sie mit dem **ccs** Befehl konfigurieren, ist die primäre Fencing-Methode, die zweite von Ihnen konfigurierte Methode ist die Backup-Fencing-Methode. Um die Reihenfolge zu ändern, können Sie die primäre Fencing-Methode aus der Konfigurationsdatei löschen und diese Methode anschließend wieder hinzufügen.

Beachten Sie, dass Sie sich jederzeit eine Liste der aktuell für einen Knoten konfigurierten Fencing-Methoden und -Instanzen anzeigen lassen können, indem Sie den folgenden Befehl ausführen. Wenn Sie keinen bestimmten Knoten angeben, zeigt dieser Befehl die aktuell für alle Knoten konfigurierten Fencing-Methoden und -Instanzen an.

```
ccs -h host --lsfenceinst [node]
```

Verwenden Sie folgendes Verfahren, um einen Knoten mit einem primären Fencing-Gerät zu konfigurieren, das ein Fencing-Gerät namens **my_apc** verwendet, welches wiederum den **fence_apc** Fencing-Agenten verwendet, sowie ein Backup-Fencing-Gerät, das ein Fencing-Gerät namens **sanswitch1** verwendet, welches wiederum den **fence_sanbox2** Fencing-Agenten verwendet. Da es sich bei dem **sanswitch1** Gerät um einen Speicher Fencing-Agent handelt, müssen Sie für dieses Gerät zusätzlich Unfencing konfigurieren.

1. Fügen Sie eine primäre Fencing-Methode für den Knoten hinzu und geben Sie einen Namen für die Fencing-Methode an.

   ```
   ccs -h host --addmethod method node
   ```

   Um beispielsweise eine Fencing-Methode namens **APC** als primäre Methode für den Knoten **node-01.example.com** in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, führen Sie folgenden Befehl aus:

   ```
   ccs -h node01.example.com --addmethod APC node01.example.com
   ```

2. Fügen Sie eine Fencing-Instanz für die primäre Methode hinzu. Sie müssen das zu verwendende Fencing-Gerät für den Knoten spezifizieren, sowie den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, und jegliche Optionen, die spezifisch für diesen Knoten sind:

   ```
   ccs -h host --addfenceinst fencedevicename node method [options]
   ```

   Um beispielsweise eine Fencing-Instanz in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, die den APC Switch Power-Port 1 auf dem Fencing-Gerät namens **my_apc** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung der Methode namens **APC** abzugrenzen, verwenden Sie folgenden Befehl:

   ```
   ccs -h node01.example.com --addfenceinst my_apc node01.example.com APC
   port=1
   ```

3. Fügen Sie eine Backup-Fencing-Methode für den Knoten hinzu und geben Sie einen Namen für die Fencing-Methode an.

   ```
   ccs -h host --addmethod method node
   ```

   Um beispielsweise eine Backup-Fencing-Methode namens **SAN** für den Knoten **node-01.example.com** in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, führen Sie folgenden Befehl aus:

```
ccs -h node01.example.com --addmethod SAN  node01.example.com
```

4. Fügen Sie eine Fencing-Instanz für die Backup-Methode hinzu. Sie müssen das zu verwendende Fencing-Gerät für den Knoten spezifizieren, sowie den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, und jegliche Optionen, die spezifisch für diesen Knoten sind:

```
ccs -h host --addfenceinst fencedevicename node method [options]
```

Um beispielsweise eine Fencing-Instanz in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** zu konfigurieren, die den SAN Switch Power-Port 11 auf dem Fencing-Gerät namens **sanswitch1** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung der Methode namens **SAN** abzugrenzen, verwenden Sie folgenden Befehl:

```
ccs -h node01.example.com --addfenceinst sanswitch1 node01.example.com SAN
port=11
```

5. Da es sich bei dem **sanswitch1** Gerät um ein Speicher-Fencing-Gerät handelt, müssen Sie für dieses Gerät zusätzlich Unfencing konfigurieren.

```
ccs -h node01.example.com --addunfence sanswitch1 node01.example.com port=11
action=on
```

Sie können nach Bedarf weitere Fencing-Methoden hinzufügen.

Dieses Verfahren konfiguriert ein Fencing-Gerät und ein Backup-Fencing-Gerät für einen Knoten im Cluster. Sie müssen das Fencing für die anderen Knoten im Cluster auf die gleiche Weise konfigurieren.

Beispiel 5.4, „**cluster.conf** nach Hinzufügen von Backup-Fencing-Methoden“ zeigt eine **cluster.conf** Konfigurationsdatei, nachdem Sie eine primäre Power-Fencing-Methode und eine Speicher-Backup-Fencing-Methode zu jedem Knoten im Cluster hinzugefügt haben.

Beispiel 5.4. `cluster.conf` nach Hinzufügen von Backup-Fencing-Methoden

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="my_apc" port="1"/>
             </method>
            <method name="SAN">
       <device name="sanswitch1" port="11"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="11" action="on"/>
         </unfence
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="my_apc" port="2"/>
            </method>
            <method name="SAN">
       <device name="sanswitch1" port="12"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="12" action="on"/>
         </unfence
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="my_apc" port="3"/>
            </method>
            <method name="SAN">
       <device name="sanswitch1" port="13"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="13" action="on"/>
         </unfence
     </clusternode>
   </clusternodes>
   <fencedevices>
        <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="my_apc" passwd="password_example"/>
        <fencedevice agent="fence_sanbox2" ipaddr="san_ip_example"
login="login_example" name="sanswitch1" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“ beschrieben.



Anmerkung

Die Reihenfolge, in der das System die konfigurierten Fencing-Methoden einsetzt, entspricht ihrer Reihenfolge in der Cluster-Konfigurationsdatei. Die erste Methode, die Sie konfigurieren, ist die primäre Fencing-Methode, die zweite von Ihnen konfigurierte Methode ist die Backup-Fencing-Methode. Um die Reihenfolge zu ändern, können Sie die primäre Fencing-Methode aus der Konfigurationsdatei löschen und diese Methode anschließend wieder hinzufügen.

5.7.4. Konfiguration eines Knotens mit redundanter Stromversorgung

Falls Ihr Cluster mit redundanter Stromversorgung für Ihre Knoten ausgestattet ist, vergewissern Sie sich, dass Ihr Fencing derart konfiguriert ist, dass Ihre Knoten bei der Abgrenzung vollständig abgeschaltet werden. Falls Sie jede Stromversorgung als separate Fencing-Methode konfigurieren, wird jede Stromversorgung separat abgegrenzt; die zweite Stromversorgung ermöglicht es dem System, weiterhin zu laufen, selbst wenn die erste Stromversorgung abgegrenzt ist, so dass das System selbst im Endeffekt nicht abgegrenzt wird. Um ein System mit dualer Stromversorgung zu konfigurieren, müssen Sie Ihre Fencing-Geräte so konfigurieren, dass beide Stromversorgungen abgeschaltet werden und somit auch das System vollständig abgeschaltet wird. Dazu ist es notwendig, dass Sie zwei Instanzen innerhalb einer einzelnen Fencing-Methode konfigurieren, und dass Sie für jede Instanz beide Fencing-Geräte mit dem **`action`** Parameter **`off`** konfigurieren, bevor Sie anschließend jedes der Geräte mit dem **`action`** Parameter **`on`** konfigurieren.

Um das Fencing für einen Knoten mit dualer Stromversorgung zu konfigurieren, folgen Sie den Schritten in diesem Abschnitt.

1. Bevor Sie das Fencing für einen Knoten mit redundanter Stromversorgung konfigurieren können, müssen Sie jeden der Netzschalter als Fencing-Gerät für den Cluster konfigurieren. Informationen über die Konfiguration von Fencing-Geräten finden Sie in Abschnitt 5.5, „Konfigurieren von Fencing-Geräten“.

   Um eine Liste aller derzeit für Ihren Cluster konfigurierten Fencing-Geräte auszugeben, führen Sie den folgenden Befehl aus:

   ```
   ccs -h host --lsfencedev
   ```

2. Fügen Sie eine Fencing-Methode für den Knoten hinzu und geben Sie einen Namen für die Fencing-Methode an.

   ```
   ccs -h host --addmethod method node
   ```

   Um beispielsweise eine Fencing-Methode namens **`APC-dual`** für den Knoten **`node-01.example.com`** in der Konfigurationsdatei auf dem Cluster-Knoten **`node-01.example.com`** zu konfigurieren, führen Sie den folgenden Befehl aus:

   ```
   ccs -h node01.example.com --addmethod APC-dual node01.example.com
   ```

3. Fügen Sie eine Fencing-Instanz für die erste Stromversorgung zur Fencing-Methode hinzu. Sie müssen angeben, welches Fencing-Gerät für den Knoten verwendet werden soll, den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, sowie jegliche Optionen für diese Methode speziell für diesen Knoten. Konfigurieren Sie an diesem Punkt den **`action`** Parameter als **`off`**.

   ```
   ccs -h host --addfenceinst fencedevicename node method [options] action=off
   ```

   Um beispielsweise in der Konfigurationsdatei auf dem Cluster-Knoten **`node-01.example.com`** eine Fencing-Instanz zu konfigurieren, die den APC Switch Power Port 1 auf dem Fencing-Gerät namens **`apc1`** verwendet, um den Cluster-Knoten **`node-01.example.com`** unter Verwendung

der Methode namens **APC-dual** abzugrenzen und um den **action** Parameter auf **off** zu setzen, führen Sie den folgenden Befehl aus:

```
ccs -h node01.example.com --addfenceinst apc1 node01.example.com APC-dual
port=1 action=off
```

4. Fügen Sie eine Fencing-Instanz für die zweite Stromversorgung zur Fencing-Methode hinzu. Sie müssen angeben, welches Fencing-Gerät für den Knoten verwendet werden soll, den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, sowie jegliche Optionen für diese Methode speziell für diesen Knoten. Konfigurieren Sie an diesem Punkt auch für diese Instanz den **action** Parameter als **off**.

```
ccs -h host --addfenceinst fencedevicename node method [options] action=off
```

Um beispielsweise in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** eine zweite Fencing-Instanz zu konfigurieren, die den APC Switch Power Port 1 auf dem Fencing-Gerät namens **apc2** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung derselben Methode wie für die erste Instanz namens **APC-dual** abzugrenzen und um den **action** Parameter auf **off** zu setzen, führen Sie den folgenden Befehl aus:

```
ccs -h node01.example.com --addfenceinst apc2 node01.example.com APC-dual
port=1 action=off
```

5. Fügen Sie nun eine weitere Fencing-Instanz für die erste Stromversorgung zur Fencing-Methode hinzu und konfigurieren Sie den **action** Parameter auf **on**. Sie müssen angeben, welches Fencing-Gerät für den Knoten verwendet werden soll, den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, sowie jegliche Optionen für diese Methode speziell für diesen Knoten, und setzen Sie den **action** Parameter auf **on**:

```
ccs -h host --addfenceinst fencedevicename node method [options] action=on
```

Um beispielsweise in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** eine Fencing-Instanz zu konfigurieren, die den APC Switch Power Port 1 auf dem Fencing-Gerät namens **apc1** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung der Methode namens **APC-dual** abzugrenzen und um den **action** Parameter auf **on** zu setzen, führen Sie den folgenden Befehl aus:

```
ccs -h node01.example.com --addfenceinst apc1 node01.example.com APC-dual
port=1 action=on
```

6. Fügen Sie eine weitere Fencing-Instanz für die zweite Stromversorgung zur Fencing-Methode hinzu und konfigurieren Sie den **action** Parameter für diese Instanz auf **on**. Sie müssen angeben, welches Fencing-Gerät für den Knoten verwendet werden soll, den Knoten, auf den diese Instanz angewendet wird, den Namen der Methode, sowie jegliche Optionen für diese Methode speziell für diesen Knoten, und setzen Sie den **action** Parameter auf **on**:

```
ccs -h host --addfenceinst fencedevicename node method [options] action=on
```

Um beispielsweise in der Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** eine zweite Fencing-Instanz zu konfigurieren, die den APC Switch Power Port 1 auf dem Fencing-Gerät namens **apc2** verwendet, um den Cluster-Knoten **node-01.example.com** unter Verwendung derselben Methode wie für die erste Instanz namens **APC-dual** abzugrenzen und um den **action** Parameter auf **on** zu setzen, führen Sie den folgenden Befehl aus:

```
ccs -h node01.example.com --addfenceinst apc2 node01.example.com APC-dual
port=1 action=on
```

Beispiel 5.5, „**cluster.conf** nach Hinzufügen von Fencing für duale Stromversorgung“ zeigt eine **cluster.conf** Konfigurationsdatei, nachdem Sie Fencing für zwei Stromversorgungen für jeden Knoten im Cluster hinzugefügt haben.

Beispiel 5.5. cluster.conf nach Hinzufügen von Fencing für duale Stromversorgung

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC-dual">
              <device name="apc1" port="1"action="off"/>
              <device name="apc2" port="1"action="off"/>
              <device name="apc1" port="1"action="on"/>
              <device name="apc2" port="1"action="on"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC-dual">
              <device name="apc1" port="2"action="off"/>
              <device name="apc2" port="2"action="off"/>
              <device name="apc1" port="2"action="on"/>
              <device name="apc2" port="2"action="on"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC-dual">
              <device name="apc1" port="3"action="off"/>
              <device name="apc2" port="3"action="off"/>
              <device name="apc1" port="3"action="on"/>
              <device name="apc2" port="3"action="on"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
       <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc1" passwd="password_example"/>
       <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc2" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“ beschrieben.

5.7.5. Entfernen von Fencing-Methoden und Fencing-Instanzen

Um eine Fencing-Methode aus Ihrer Cluster-Konfiguration zu entfernen, führen Sie den folgenden Befehl aus:

```
ccs -h host --rmmethod method node
```

Um beispielsweise eine Fencing-Methode namens **APC**, die Sie für **node01.example.com** konfiguriert hatten, aus der Cluster-Konfigurationsdatei auf dem Cluster-Knoten **node01.example.com** zu entfernen, führen Sie den folgenden Befehl aus:

```
ccs -h node01.example.com  --rmmethod APC node01.example.com
```

Um alle Fencing-Instanzen eines Fencing-Geräts von einer Fencing-Methode zu entfernen, führen Sie den folgenden Befehl aus:

```
ccs -h host --rmfenceinst fencedevicename node method
```

Um beispielsweise alle Instanzen des Fencing-Geräts namens **apc1** von der Methode namens **APC-dual**, konfiguriert für **node01.example.com**, aus der Cluster-Konfigurationsdatei auf dem Cluster-Knoten **node01.example.com** zu entfernen, führen Sie den folgenden Befehl aus:

```
ccs -h node01.example.com --rmfenceinst apc1 node01.example.com APC-dual
```

5.8. Konfigurieren einer Ausfallsicherungs-Domain

Eine Ausfallsicherungs-Domain ist eine benannte Teilmenge von Cluster-Knoten, die dazu berechtigt ist, einen Cluster-Dienst im Falle eines Knotenausfalls weiterzuführen. Eine Ausfallsicherungs-Domain kann die folgenden Charakteristiken haben:

- Uneingeschränkt — Ermöglicht Ihnen, eine Teilmenge bevorzugter Mitglieder zu spezifizieren, doch der dieser Domain zugewiesene Cluster-Dienst kann auf jedem verfügbaren Mitglied ausgeführt werden.
- Eingeschränkt — Ermöglicht Ihnen, die Mitglieder einzuschränken, auf denen ein bestimmter Cluster-Dienst laufen darf. Falls keines der Mitglieder in einer eingeschränkten Ausfallsicherungs-Domain verfügbar ist, kann der Cluster-Dienst nicht gestartet werden (weder manuell noch durch die Cluster-Software).
- Ungeordnet — Wenn ein Cluster-Dienst einer ungeordneten Ausfallsicherungs-Domain zugewiesen ist, wird das Mitglied, auf dem der Cluster-Dienst ausgeführt wird, ohne Berücksichtigung von Prioritäten aus den verfügbaren Mitgliedern der Ausfallsicherungs-Domain ausgewählt.
- Geordnet — Ermöglicht Ihnen, eine Prioritätsreihenfolge für die Mitglieder einer Ausfallsicherungs-Domain anzugeben. Das erste Mitglied in der Liste wird bevorzugt, gefolgt vom zweiten Mitglied in der Liste, usw.
- Failback — Ermöglicht Ihnen festzulegen, ob ein Dienst in der Ausfallsicherungs-Domain auf den Knoten zurückwechseln soll, auf dem er vor dessen Ausfall ursprünglich ausgeführt wurde. Das Konfigurieren dieser Charakteristik ist hilfreich in Situationen, in denen ein Knoten häufig ausfällt und Teil einer geordneten Ausfallsicherungs-Domain ist. In diesem Fall würde ein Dienst, der auf dem bevorzugten Knoten in einer Ausfallsicherungs-Domain läuft, möglicherweise wiederholt zwischen dem bevorzugten Knoten und einem anderen Knoten hin- und herwechseln, was beträchtliche Leistungseinbußen zur Folge hätte.



Anmerkung

Die Failback-Charakteristik greift nur, wenn die geordnete Ausfallsicherung konfiguriert ist.



Anmerkung

Eine Änderung der Ausfallsicherungs-Domain-Konfiguration hat keine Auswirkungen auf derzeit laufende Dienste.



Anmerkung

Ausfallsicherungs-Domains werden für den Betrieb *nicht* benötigt.

Standardmäßig sind Ausfallsicherungs-Domains uneingeschränkt und ungeordnet.

In einem Cluster mit mehreren Mitgliedern kann Ihnen der Einsatz einer beschränkten Ausfallsicherungs-Domain die Arbeit erleichtern. Denn um einen Cluster zum Ausführen eines Cluster-Dienstes (wie z.B. **httpd**) einzurichten, müssen Sie auf allen Cluster-Mitgliedern, die diesen Cluster-Dienst ausführen sollen, eine identische Konfiguration einrichten. Anstatt den gesamten Cluster zur Ausführung dieses Cluster-Dienstes einzurichten, müssen Sie somit nur die Mitglieder der beschränkten Ausfallsicherungs-Domain, die Sie mit diesem Cluster-Dienst verknüpfen möchten, entsprechend einrichten.



Anmerkung

Um ein bevorzugtes Mitglied zu konfigurieren, können Sie eine uneingeschränkte Ausfallsicherungs-Domain einrichten, die nur aus einem Cluster-Mitglied besteht. Dadurch läuft der Cluster-Dienst zwar hauptsächlich auf diesem einen Cluster-Mitglied (dem bevorzugten Mitglied), doch erlaubt es dem Cluster-Dienst gleichzeitig, im Falle eines Ausfalls auf einen beliebigen anderen Knoten zu wechseln.

Um eine Ausfallsicherungs-Domain zu konfigurieren, wenden Sie folgendes Verfahren an:

1. Um eine Ausfallsicherungs-Domain hinzuzufügen, führen Sie den folgenden Befehl aus:

```
ccs -h host --addfailoverdomain name [restricted] [ordered] [nofailback]
```



Anmerkung

Der Name sollte aussagekräftig genug sein, um daraus im Vergleich zu anderen Namen im Cluster auf den Zweck schließen zu können.

Beispielsweise konfiguriert der folgende Befehl eine Ausfallsicherungs-Domain namens **example_pri** auf **node-01.example.com**, die uneingeschränkt und geordnet ist und Failback erlaubt:

```
ccs -h node-01.example.com --addfailoverdomain example_pri ordered
```

2. Um einen Knoten zu einer Ausfallsicherungs-Domain hinzuzufügen, führen Sie den folgenden Befehl aus:

```
ccs -h host --addfailoverdomainnode failoverdomain node priority
```

Um beispielsweise die Ausfallsicherungs-Domain **example_pri** in der Konfigurationsdatei auf **node-01.example.com** so zu konfigurieren, dass sie **node-01.example.com** mit der Priorität 1, **node-02.example.com** mit der Priorität 2 und **node-03.example.com** mit der

Priorität 3 beinhaltet, führen Sie die folgenden Befehle aus:

```
ccs -h node-01.example.com --addfailoverdomainnode example_pri node-
01.example.com 1
ccs -h node-01.example.com --addfailoverdomainnode example_pri node-
02.example.com 2
ccs -h node-01.example.com --addfailoverdomainnode example_pri node-
03.example.com 3
```

Sie können sich mithilfe des folgenden Befehls eine Liste aller in einem Cluster konfigurierten Ausfallsicherungs-Domains und Ausfallsicherungs-Domain-Knoten anzeigen lassen:

```
ccs -h host --lsfailoverdomain
```

Um eine Ausfallsicherungs-Domain zu entfernen, führen Sie den folgenden Befehl aus:

```
ccs -h host --rmfailoverdomain name
```

Um einen Knoten aus einer Ausfallsicherungs-Domain zu entfernen, führen Sie den folgenden Befehl aus:

```
ccs -h host --rmfailoverdomainnode failoverdomain node
```

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“ beschrieben.

5.9. Konfigurieren von globalen Cluster-Ressourcen

Sie können zwei Arten von Ressourcen konfigurieren:

- Global — Ressourcen, die jedem Dienst im Cluster zur Verfügung stehen.
- Dienstspezifisch — Ressourcen, die nur einem Dienst zur Verfügung stehen.

Um eine Liste der derzeit konfigurierten Ressourcen und Dienste im Cluster zu sehen, führen Sie den folgenden Befehl aus:

```
ccs -h host --lsservices
```

Um eine globale Cluster-Ressource hinzuzufügen, führen Sie den folgenden Befehl aus. Sie können eine Ressource lokal für einen bestimmten Dienst hinzufügen, während Sie diesen Dienst konfigurieren, wie in Abschnitt 5.10, „Hinzufügen eines Cluster-Dienstes zum Cluster“ beschrieben.

```
ccs -h host --addresource resourcetype [resource options]
```

Beispielsweise fügt der folgende Befehl eine globale Dateisystem-Ressource zur Cluster-Konfigurationsdatei auf **node01.example.com** hinzu. Der Name der Ressource lautet **web_fs**, das Dateisystemgerät ist **/dev/sdd2**, der Einhängepunkt des Dateisystems ist **/var/www**, und der Dateisystemtyp ist **ext3**.

```
ccs -h node01.example.com --addresource fs name=web_fs device=/dev/sdd2
mountpoint=/var/www fstype=ext3
```

Für Informationen über die verfügbaren Ressourcentypen und Ressourcenoptionen siehe Anhang B, *Parameter der Hochverfügbarkeitsressourcen*.

Um eine globale Ressource zu löschen, führen Sie den folgenden Befehl aus:

```
ccs -h host --rmresource resourcetype [resource options]
```

Falls Sie die Parameter einer vorhandenen, globalen Ressource ändern müssen, können Sie die Ressourcen entfernen und sie erneut konfigurieren.

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“ beschrieben.

5.10. Hinzufügen eines Cluster-Dienstes zum Cluster

Um einen Cluster-Dienst in einem Cluster zu konfigurieren, führen Sie die folgenden Schritte aus:

1. Fügen Sie mit den folgenden Befehl einen Dienst zum Cluster hinzu:

```
ccs -h host --addservice servicename [service options]
```



Anmerkung

Der Name sollte aussagekräftig genug sein, um den Dienst klar von anderen Diensten im Cluster unterscheiden zu können.

Wenn Sie einen Dienst zur Cluster-Konfiguration hinzufügen, können Sie die folgenden Parameter konfigurieren:

- **autostart** — Legt fest, ob der Dienst beim Start des Clusters automatisch gestartet werden soll. Verwenden Sie "1" zur Aktivierung und "0" zur Deaktivierung; standardmäßig ist er aktiviert.
- **domain** — Legt eine Ausfallsicherungs-Domain fest (falls erforderlich).
- **exclusive** — Legt eine Richtlinie fest, gemäß der dieser Dienst ausschließlich auf Knoten ausgeführt werden darf, auf denen kein anderer Dienst läuft.
- **recovery** — Legt eine Richtlinie zur Wiederherstellung für den Dienst fest. Mögliche Optionen sind "relocate" (Verlegung), "restart" (Neustart), "restart-disable" (Neustart-Deaktivierung) oder "disable" (Deaktivierung). Mit der "restart"-Wiederherstellungsrichtlinie versucht das System einen Neustart des ausgefallenen Dienstes, bevor es den Dienst auf einen anderen Knoten zu verlegen versucht. Mit der "relocate"-Wiederherstellungsrichtlinie versucht das System einen Neustart des Dienstes auf einem anderen Knoten. Mit der "disable"-Wiederherstellungsrichtlinie deaktiviert das System die Ressourcengruppe, falls eine der Komponenten ausfällt. Mit der "restart-disable"-Wiederherstellungsrichtlinie versucht das System einen Neustart des ausgefallenen Dienstes an demselben Ort. Scheitert dieser Versuch, wird der Dienst deaktiviert, statt auf einen anderen Host im Cluster verlegt zu werden.

  Falls Sie **Restart** oder **Restart-Disable** als Wiederherstellungsrichtlinie für diesen Dienst auswählen, können Sie die maximale Anzahl an Neustartfehlschlägen festlegen, bevor der Dienst verlegt oder deaktiviert wird, sowie die Zeitspanne in Sekunden, nach der ein Neustart nicht weiter versucht werden soll.

Um beispielsweise einen Dienst namens **example_apache** zur Konfigurationsdatei auf dem Cluster-Knoten **node-01.example.com** hinzuzufügen, der die Ausfallsicherungs-Domain **example_pri** benutzt und die Wiederherstellungsrichtlinie **relocate** verwendet, führen Sie den folgenden Befehl aus:

```
ccs -h node-01.example.com --addservice example_apache domain=example_pri
recovery=relocate
```

Bei der Konfiguration von Diensten für einen Cluster kann es hilfreich sein, eine Liste der Dienste

zu sehen, die für Ihren Cluster zur Verfügung stehen, sowie die jeweiligen Optionen, die für diese Dienste verfügbar sind. Für mehr Informationen über die Verwendung von **ccs**, um eine Liste verfügbarer Dienste und Optionen anzuzeigen, werfen Sie einen Blick auf Abschnitt 5.11, „Anzeigen verfügbarer Cluster-Dienste und -Ressourcen“.

2. Fügen Sie mit dem folgenden Befehl Ressourcen zu diesem Dienst hinzu:

```
ccs -h host --addsubservice servicename subservice [service options]
```

Bestücken Sie den Dienst abhängig von dem Ressourcentyp, den Sie verwenden möchten, entweder mit globalen oder dienstspezifischen Ressourcen. Um eine globale Ressource hinzuzufügen, verwenden Sie die **--addsubservice** Option von **ccs**. Um beispielsweise die globale Dateisystemressource namens **web_fs** zu dem Dienst namens **example_apache** in der Cluster-Konfigurationsdatei auf **node-01.example.com** hinzuzufügen, führen Sie den folgenden Befehl aus:

```
ccs -h node01.example.com --addsubservice example_apache fs ref=web_fs
```

Um eine dienstspezifische Ressource zum Dienst hinzuzufügen, müssen Sie sämtliche Dienstoptionen angeben. Falls Sie beispielsweise **web_fs** nicht bereits als globalen Dienst definiert haben, können Sie es mithilfe des folgenden Befehls als dienstspezifische Ressource hinzufügen:

```
ccs -h node01.example.com --addsubservice example_apache fs name=web_fs
device=/dev/sdd2 mountpoint=/var/www fstype=ext3
```

3. Um einen untergeordneten Dienst zu diesem Dienst hinzuzufügen, verwenden Sie zudem die **--addsubservice** Option des **ccs** Befehls und geben dabei die Dienstoptionen an.

Falls Sie einen Dienst innerhalb einer Baumstruktur von Abhängigkeiten hinzufügen müssen, verwenden Sie einen Doppelpunkt (":"), um Elemente voneinander zu trennen, und Klammern, um untergeordnete Dienste desselben Typs zu identifizieren. Das folgende Beispiel fügt einen dritten **nfsclient** Dienst als untergeordneten Dienst eines **nfsclient** Dienstes hinzu, der selbst ein untergeordneter Dienst eines **nfsclient** Dienstes ist, der selbst wiederum ein untergeordneter Dienst eines Dienstes namens **service_a** ist:

```
ccs -h node01.example.com --addsubservice service_a
nfsclient[1]:nfsclient[2]:nfsclient
```



Anmerkung

Falls Sie eine Samba-Dienst Ressource hinzufügen, fügen Sie diese direkt zum Dienst hinzu, *nicht* als Kind einer anderen Ressource.



Anmerkung

Wenn Sie einen Abhängigkeitenbaum für einen Cluster-Dienst konfigurieren, der eine IP-Adress-Ressource enthält, deren IP-Adresse geändert werden darf ("Floating"), müssen Sie die IP-Ressource als ersten Eintrag konfigurieren.



Anmerkung

Um die Existenz der in einem Cluster-Dienst verwendeten IP-Service-Ressourcen zu überprüfen, können Sie den **`/sbin/ip addr show`** Befehl auf einem Cluster-Knoten verwenden (anstelle des überholten **`ifconfig`** Befehls). Die folgende Ausgabe zeigt den **`/sbin/ip addr show`** Befehl auf einem Knoten ausgeführt auf dem ein Cluster-Dienst läuft:

```
1: lo: <LOOPBACK,UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP> mtu 1356 qdisc pfifo_fast qlen 1000
    link/ether 00:05:5d:9a:d8:91 brd ff:ff:ff:ff:ff:ff
    inet 10.11.4.31/22 brd 10.11.7.255 scope global eth0
    inet6 fe80::205:5dff:fe9a:d891/64 scope link
    inet 10.11.4.240/22 scope global secondary eth0
       valid_lft forever preferred_lft forever
```

Um einen Dienst samt aller zugehörigen untergeordneten Dienste zu entfernen, führen Sie den folgenden Befehl aus:

```
ccs -h host --rmservice servicename
```

Führen Sie den folgenden Befehl aus, um einen untergeordneten Dienst zu entfernen:

```
ccs -h host --rmsubservice servicename subservice [service options]
```

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“ beschrieben.

5.11. Anzeigen verfügbarer Cluster-Dienste und -Ressourcen

Sie können den **`ccs`** Befehl verwenden, um eine Liste aller verfügbaren Ressourcen und Dienste für einen Cluster anzuzeigen. Auch können Sie mit dem **`ccs`** Befehl eine Liste aller Optionen anzeigen, die Sie für einen bestimmten Dienst- oder Ressourcentyp spezifizieren können.

Um eine Liste aller derzeit für Ihren Cluster verfügbaren Cluster-Dienste anzuzeigen, führen Sie einen der folgenden Befehle aus (**`--lsresourceopts`** ist ein Alias für **`--lsserviceopts`**):

```
ccs -h host --lsserviceopts
ccs -h host --lsresourceopts
```

Beispielsweise zeigt der folgende Befehl die Cluster-Dienste und Ressourcen, die auf dem Cluster-Knoten **`node1`** verfügbar sind.

```
[root@ask-03 ~]# ccs -h node1 --lsserviceopts
service - Defines a service (resource group).
ASEHAagent - Sybase ASE Failover Instance
SAPDatabase - SAP database resource agent
SAPInstance - SAP instance resource agent
apache - Defines an Apache web server
clusterfs - Defines a cluster file system mount.
fs - Defines a file system mount.
ip - This is an IP address.
lvm - LVM Failover script
mysql - Defines a MySQL database server
named - Defines an instance of named server
netfs - Defines an NFS/CIFS file system mount.
nfsclient - Defines an NFS client.
nfsexport - This defines an NFS export.
nfsserver - This defines an NFS server resource.
openldap - Defines an Open LDAP server
oracledb - Oracle 10g Failover Instance
orainstance - Oracle 10g Failover Instance
oralistener - Oracle 10g Listener Instance
postgres-8 - Defines a PostgreSQL server
samba - Dynamic smbd/nmbd resource agent
script - LSB-compliant init script as a clustered resource.
tomcat-6 - Defines a Tomcat server
vm - Defines a Virtual Machine
action - Overrides resource action timings for a resource instance.
```

Führen Sie den folgenden Befehl aus, um eine Liste aller Optionen anzuzeigen, die Sie für einen bestimmten Diensttyp spezifizieren können:

```
ccs -h host --lsserviceopts service_type
```

Beispielsweise zeigt der folgende Befehl die Dienstoptionen, die für den **vm** Dienst verfügbar sind.

```
[root@ask-03 ~]# ccs -f node1 --lsserviceopts vm
vm - Defines a Virtual Machine
  Required Options:
    name: Name
  Optional Options:
    domain: Cluster failover Domain
    autostart: Automatic start after quorum formation
    exclusive: Exclusive resource group
    recovery: Failure recovery policy
    migration_mapping: memberhost:targethost,memberhost:targethost ..
    use_virsh: If set to 1, vm.sh will use the virsh command to manage virtual
machines instead of xm. This is required when using non-Xen virtual machines (e.g.
qemu / KVM).
    xmlfile: Full path to libvirt XML file describing the domain.
    migrate: Migration type (live or pause, default = live).
    path: Path to virtual machine configuration files.
    snapshot: Path to the snapshot directory where the virtual machine image will
be stored.
    depend: Top-level service this depends on, in service:name format.
    depend_mode: Service dependency mode (soft or hard).
    max_restarts: Maximum restarts for this service.
    restart_expire_time: Restart expiration time; amount of time before a restart
is forgotten.
    status_program: Additional status check program
    hypervisor: Hypervisor
    hypervisor_uri: Hypervisor URI (normally automatic).
    migration_uri: Migration URI (normally automatic).
    __independent_subtree: Treat this and all children as an independent subtree.
    __enforce_timeouts: Consider a timeout for operations as fatal.
    __max_failures: Maximum number of failures before returning a failure to a
status check.
    __failure_expire_time: Amount of time before a failure is forgotten.
    __max_restarts: Maximum number restarts for an independent subtree before
giving up.
    __restart_expire_time: Amount of time before a failure is forgotten for an
independent subtree.
```

5.12. Virtuelle Maschinen-Ressourcen

Virtuelle Maschinen-Ressourcen werden anders konfiguriert als andere Cluster-Ressourcen. Insbesondere werden sie nicht in Dienst-Definitionen gruppiert. Ab der Red Hat Enterprise Linux 6.2 Release können Sie bei der Konfiguration einer virtuellen Maschine in einem Cluster mit dem **ccs** Befehl die Option **--addvm** verwenden (statt der **addservice** Option). Dadurch wird gewährleistet, dass die **vm** Ressource direkt unter dem **rm** Konfigurationsknoten in der Cluster-Konfigurationsdatei definiert wird.

Eine virtuelle Maschinen-Ressource erfordert mindestens einen **name** und einen **path** Parameter. Der **name** Parameter sollte dem Namen der **libvirt** Domain entsprechen und der **path** Parameter sollte das Verzeichnis spezifizieren, in dem die virtuellen Maschinen-Definitionen gespeichert sind.



Anmerkung

Der **path** Parameter in der Cluster-Konfigurationsdatei ist eine Pfadspezifikation oder ein Verzeichnisname, kein Pfad zu einer einzelnen Datei.

Angenommen, virtuelle Maschinen-Definitionen befinden Sie auf einem gemeinsam genutzten Verzeichnis namens **/mnt/vm_defs**, dann definiert der folgende Befehl eine virtuelle Maschine namens **guest1**:

```
# ccs -h node1.example.com --addvm guest1 path=/mnt/vm_defs
```

Durch Ausführen dieses Befehls wird die folgende Zeile zum **rm** Konfigurationsknoten in der **cluster.conf** Datei hinzugefügt:

```
<vm name="guest1" path="/mnt/vm_defs"/>
```

5.13. Konfigurieren eines Quorumdatenträgers



Wichtig

Die Parameter und Heuristiken des Quorumdatenträgers hängen von der jeweiligen Umgebung und ggf. besonderen Anforderungen ab. Um die Parameter und Heuristiken des Quorumdatenträgers zu verstehen, werfen Sie einen Blick auf die qdisk(5) Handbuchseite. Falls Sie Hilfe zum Verständnis oder zur Verwendung von Quorumdatenträgern benötigen, setzen Sie sich bitte mit einem autorisierten Red Hat Support-Vertreter in Verbindung.

Verwenden Sie den folgenden Befehl, um Ihr System zur Verwendung eines Quorumdatenträgers zu konfigurieren:

```
ccs -h host --setquorumd [quorumd options]
```

Beachten Sie, dass dieser Befehl alle anderen Eigenschaften, die Sie mit der **--setquorumd** Option erstellen können, auf die Standardwerte zurücksetzt, wie in Abschnitt 5.1.5, „Befehle, die vorhergehende Einstellungen überschreiben“ beschrieben.

Tabelle 5.1, „Optionen des Quorumdatenträgers“ fasst die Bedeutung der Quorumdatenträgeroptionen zusammen, die Sie ggf. festlegen müssen. Eine vollständige Liste der Quorumdatenträgerparameter finden Sie im Cluster-Schema unter **/usr/share/cluster/cluster.rng** sowie im kommentierten Schema unter **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html**.

Tabelle 5.1. Optionen des Quorumdatenträgers

Parameter	Beschreibung
interval	Die Häufigkeit von Lese-/Schreibzyklen in Sekunden.
votes	Die Anzahl der Stimmen, die der Quorum-Daemon an **cman** mitteilt, wenn eine Punktzahl erreicht wird, die hoch genug ist.
tko	Die Anzahl von Zyklen, die ein Knoten auslassen muss, bevor dieser für "tot" erklärt wird.
min_score	Die Mindestpunktzahl eines Knotens, bei der dieser noch als "lebendig" betrachtet wird. Falls dieser Wert weggelassen oder auf 0 gesetzt wird, so wird die Standardfunktion **floor((*n*+1)/2)** verwendet, wobei ***n*** die Summe der Heuristik-Punktzahlen ist. Der **Minimum Score** Wert darf nie die Summe der Heuristik-Punktzahlen übersteigen, andernfalls wird der Quorumdatenträger nicht verfügbar sein.
device	Das vom Quorum-Daemon verwendete Speichergerät. Das Gerät muss auf allen Knoten dasselbe sein.
label	Spezifiziert die Kennung des Quorumdatenträgers, die von dem **mkqdisk** Dienstprogramm erstellt wurde. Wenn dieses Feld eine Eintragung enthält, überschreibt die Kennung das **Device** Feld. Wird dieses Feld verwendet, liest der Quorum-Daemon die **/proc/partitions**, sucht nach qdisk-Signaturen auf jedem gefundenen Blockgerät und vergleicht die Kennung mit der angegebenen Kennung. Dies ist in Konfigurationen hilfreich, in denen sich der Name des Quorumgeräts von Knoten zu Knoten unterscheidet.

Verwenden Sie den folgenden Befehl, um die Heuristiken für einen Quorumdatenträger zu konfigurieren:

```
ccs -h host --addheuristic [heuristic options]
```

Tabelle 5.2, „Heuristiken des Quorumdatenträgers“ fasst die Bedeutung der Quorumdatenträgerheuristiken zusammen, die Sie ggf. erstellen müssen.

Tabelle 5.2. Heuristiken des Quorumdatenträgers

Parameter	Beschreibung
program	Der Pfad zum Programm das verwendet wird, um festzustellen, ob diese Heuristik verfügbar ist. Dies kann alles sein, was durch **/bin/sh-c** ausgeführt werden kann. Ein Rückgabewert von 0 bedeutet Erfolg, alles andere bedeutet Misserfolg. Dieses Feld ist für den Gebrauch eines Quorumdatenträgers erforderlich.
interval	Die Zeitabstände (in Sekunden), in denen die Heuristik abgefragt wird. Das standardmäßige Intervall für jede Heuristik ist 2 Sekunden.
score	Die Gewichtung dieser Heuristik. Seien Sie vorsichtig beim Festlegen der Gewichtung für Heuristiken. Die standardmäßige Gewichtung für jede Heuristik ist 1.
tko	Die Anzahl von aufeinander folgenden Fehlschlägen, bevor diese Heuristik für nicht verfügbar erklärt wird.

Um eine Liste der Optionen und Heuristiken für Quorumdatenträger anzusehen, die auf einem System konfiguriert sind, können Sie den folgenden Befehl ausführen:

```
ccs -h host --lsquorum
```

Um eine Heuristik zu entfernen, die von einer Heuristikoption spezifiziert wird, können Sie den folgenden

Befehl ausführen:

```
ccs -h host rmheuristic [heuristic options]
```

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“ beschrieben.



Anmerkung

Durch das Synchronisieren und Aktivieren wird die aktualisierte Cluster-Konfigurationsdatei verbreitet und aktiviert. Damit der Quorumdatenträger jedoch funktioniert, muss der Cluster neu gestartet werden (siehe Abschnitt 6.2, „Starten und Stoppen eines Clusters“), um sicherzustellen, dass der **qdiskd** Daemon auf jedem Knoten neu gestartet wird.

5.14. Sonstige Cluster-Konfiguration

Dieser Abschnitt beschreibt die Verwendung des **ccs** Befehls, um Folgendes zu konfigurieren:

- Abschnitt 5.14.1, „Cluster-Konfigurationsversion“
- Abschnitt 5.14.2, „Multicast-Konfiguration“
- Abschnitt 5.14.3, „Konfiguration eines Zwei-Knoten-Clusters“
- Abschnitt 5.14.4, „Protokollierung“
- Abschnitt 5.14.5, „Konfiguration des Redundant Ring Protocols“

Sie können den **ccs** Befehl auch dazu verwenden, erweiterte Cluster-Konfigurationsparameter einzustellen, wie z.B. **totem** Optionen, **dlm** Optionen, **rm** Optionen und **cman** Optionen. Für Informationen über das Erstellen dieser Parameter siehe die **ccs**(8) Handbuchseite und das kommentierte Cluster-Konfigurationsdatei Schema unter **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html**.

Um eine Liste der sonstigen Cluster-Parameter anzusehen, die für einen Cluster konfiguriert wurden, führen Sie den folgenden Befehl aus:

```
ccs -h host --lsmisc
```

5.14.1. Cluster-Konfigurationsversion

Eine Cluster-Konfigurationsdatei beinhaltet einen Konfigurationsversions-Wert. Der Konfigurationsversions-Wert wird standardmäßig auf **1** gesetzt, wenn Sie eine Cluster-Konfigurationsdatei erstellen, und wird jedes Mal automatisch erhöht, wenn Sie Ihre Cluster-Konfiguration ändern. Falls Sie jedoch einen abweichenden Wert angeben müssen, können Sie diesen mithilfe des folgenden Befehls angeben:

```
ccs -h host --setversion n
```

Sie können den aktuellen Konfigurationsversions-Wert auf einer vorhandenen Cluster-Konfigurationsdatei mit dem folgenden Befehl abrufen:

```
ccs -h host --getversion
```

Um den aktuellen Konfigurationsversions-Wert in der Cluster-Konfigurationsdatei auf jedem Knoten im Cluster um 1 zu erhöhen, führen Sie den folgenden Befehl aus:

```
ccs -h host --incversion
```

5.14.2. Multicast-Konfiguration

Falls Sie in der Cluster-Konfigurationsdatei keine Multicast-Adresse angeben, erstellt die Red Hat Hochverfügbarkeits-Add-On-Software eine Multicast-Adresse basierend auf der Cluster-ID. Es generiert die unteren 16 Bits der Adresse und fügt diese an den oberen Teil der Adresse an, abhängig davon, ob das IP-Protokoll IPv4 oder IPv6 verwendet wird:

- Bei IPv4 — Die gebildete Adresse ist 239.192. plus die von der Red Hat Hochverfügbarkeits-Add-On-Software generierten unteren 16 Bits.
- Bei IPv6 — Die gebildete Adresse ist FF15:: plus die von der Red Hat Hochverfügbarkeits-Add-On-Software generierten unteren 16 Bits.



Anmerkung

Die Cluster-ID ist eine eindeutige Kennung, die **cman** für jeden Cluster generiert. Um die Cluster-ID anzusehen, führen Sie den **cman_tool status** Befehl auf einem Cluster-Knoten durch.

Mithilfe des folgenden Befehls können Sie manuell eine Multicast-Adresse in der Cluster-Konfigurationsdatei spezifizieren:

```
ccs -h host --setmulticast multicastaddress
```

Beachten Sie, dass dieser Befehl alle anderen Eigenschaften, die Sie mit der **--setmulticast** Option erstellen können, auf die Standardwerte zurücksetzt, wie in Abschnitt 5.1.5, „Befehle, die vorhergehende Einstellungen überschreiben“ beschrieben.

Falls Sie eine Multicast-Adresse angeben, sollten Sie die 239.192.x.x Serien (oder FF15:: für IPv6) nutzen, die **cman** verwendet. Falls Sie eine Multicast-Adresse außerhalb dieses Bereichs verwenden, kann dies andernfalls zu unvorhergesehenem Verhalten führen. So könnte z.B. die Adresse 224.0.0.x (d.h. "Alle Hosts auf dem Netzwerk") unter Umständen von mancher Hardware nicht korrekt oder gar nicht geroutet werden.

Falls Sie eine Multicast-Adresse angeben oder ändern, müssen Sie den Cluster-Knoten neu starten, damit die Änderungen wirksam werden. Informationen über das Starten und Stoppen eines Clusters mit dem **ccs** Befehl finden Sie in Abschnitt 6.2, „Starten und Stoppen eines Clusters“.



Anmerkung

Falls Sie eine Multicast-Adresse angeben, überprüfen Sie die Konfiguration der Router, die von Cluster-Paketen durchquert werden. Manche Router brauchen eine lange Zeit zum Lernen von Adressen, was sich drastisch auf die Cluster-Leistung auswirken kann.

Um eine Multicast-Adresse aus einer Konfigurationsdatei zu entfernen, verwenden Sie die **--setmulticast** Option von **ccs**, geben dabei aber keine Multicast-Adresse an:

```
ccs -h host --setmulticast
```

5.14.3. Konfiguration eines Zwei-Knoten-Clusters

Falls Sie einen Zwei-Knoten-Cluster konfigurieren, können Sie den folgenden Befehl ausführen, damit es einem einzelnen Knoten möglich ist, das Quorum zu erhalten (z.B. falls der andere Knoten ausfällt):

```
ccs -h host --setcman two_node=1 expected_votes=1
```

Beachten Sie, dass dieser Befehl alle anderen Eigenschaften, die Sie mit der **--setcman** Option erstellen können, auf die Standardwerte zurücksetzt, wie in Abschnitt 5.1.5, „Befehle, die vorhergehende Einstellungen überschreiben“ beschrieben.

Falls Sie den **ccs --setcman** Befehl zum Hinzufügen, Entfernen oder Ändern der **two_node** Option verwenden, müssen Sie den Cluster-Knoten neu starten, damit die Änderungen wirksam werden. Informationen über das Starten und Stoppen eines Clusters mit dem **ccs** Befehl finden Sie in Abschnitt 6.2, „Starten und Stoppen eines Clusters“.

5.14.4. Protokollierung

Sie können Debugging für alle Daemons in einem Cluster aktivieren, oder Sie können Protokollierung für bestimmte Cluster-Prozesse aktivieren.

Um Debugging für alle Daemons zu aktivieren, führen Sie den folgenden Befehl aus. Standardmäßig wird Protokollausgabe in die Datei **/var/log/cluster/*daemon*.log** geschrieben.

```
ccs -h host --setlogging [logging options]
```

Beispielsweise aktiviert der folgende Befehl das Debugging für alle Daemons.

```
# ccs -h node1.example.com --setlogging debug=on
```

Beachten Sie, dass dieser Befehl alle anderen Eigenschaften, die Sie mit der **--setlogging** Option erstellen können, auf die Standardwerte zurücksetzt, wie in Abschnitt 5.1.5, „Befehle, die vorhergehende Einstellungen überschreiben“ beschrieben.

Um Debugging für einen einzelnen Cluster-Prozess zu aktivieren, führen Sie den folgenden Befehl aus. Die Konfiguration für einzelne Daemons setzt dabei die globalen Einstellungen außer Kraft.

```
ccs -h host --addlogging [logging daemon options]
```

Beispielsweise aktivieren die folgenden Befehle das Debugging für die **corosync** und **fenced** Daemons.

```
# ccs -h node1.example.com --addlogging name=corosync debug=on
# ccs -h node1.example.com --addlogging name=fenced debug=on
```

Verwenden Sie den folgenden Befehl, um die Protokollierungseinstellungen für einzelne Daemons zu entfernen.

```
ccs -h host --rmlogging name=clusterprocess
```

Beispielsweise entfernt der folgende Befehl die Daemon-spezifischen Protokolleinstellungen für den **fenced** Daemon.

```
ccs -h host --rmlogging name=fenced
```

Eine Liste der Daemons, für die Sie die Protokollierung aktivieren können, sowie die zusätzlichen Protokollierungsoptionen, die Sie sowohl global als auch für einzelne Daemons konfigurieren können, finden Sie auf der **cluster.conf**(5) Handbuchseite.

Vergessen Sie nicht, nach Abschluss der Konfiguration aller Komponenten Ihres Clusters die Cluster-Konfigurationsdatei auf allen Knoten zu synchronisieren, wie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“ beschrieben.

5.14.5. Konfiguration des Redundant Ring Protocols

Ab Red Hat Enterprise Linux 6.4 unterstützt das Red Hat Hochverfügbarkeits-Add-On die Konfiguration des Redundant Ring Protocols. Bei der Verwendung des Redundant Ring Protocols müssen Sie eine Vielzahl von Überlegungen berücksichtigen, wie in Abschnitt 7.6, „Konfiguration von Redundant Ring Protocol“ beschrieben.

Um eine zweite Netzwerkschnittstelle für die Verwendung des Redundant Ring Protocols festzulegen, fügen Sie einen alternativen Namen für den Knoten mit der **--addalt** Option des **ccs** Befehls hinzu:

```
ccs -h host --addalt node_name alt_name
```

Zum Beispiel konfiguriert der folgende Befehl den alternativen Namen **clusternet-node1-eth2** für den Cluster-Knoten **clusternet-node1-eth1**:

```
# ccs -h clusternet-node1-eth1 --addalt clusternet-node1-eth1 clusternet-node1-eth2
```

Optional können Sie manuell eine Multicast-Adresse, einen Port und eine TTL für den zweiten Ring angeben. Wenn Sie eine Multicast-Adresse für den zweiten Ring angeben, muss entweder die alternative Multicast-Adresse oder der alternative Port anders sein als die Multicast-Adresse für den ersten Ring. Wenn Sie einen alternativen Port angeben, müssen die Port-Nummern des ersten Rings und des zweiten Rings um mindestens zwei unterschiedlich sein, da das System selbst port und port-1 verwendet, um Operationen durchzuführen. Wenn Sie keine alternative Multicast-Adresse angeben haben, wird das System automatisch eine andere Multicast-Adresse für den zweiten Ring verwenden.

Zur Angabe einer alternativen Multicast-Addresse, eines Ports oder einer TTL für den zweiten Ring verwenden Sie die **--setaltmulticast** Option des **ccs** Befehls:

```
ccs -h host --setaltmulticast [alt_multicast_address] [alt_multicast_options].
```

Zum Beispiel legt der folgende Befehl eine alternative Multicast-Adresse 239.192.99.88, einen Port von 888 und eine TTL von 3 für den Cluster der in der **cluster.conf** Datei auf dem Knoten **clusternet-node1-eth1** definiert ist, fest:

```
ccs -h clusternet-node1-eth1 --setaltmulticast 239.192.99.88 port=888 ttl=3
```

Um eine alternative Multicast-Adresse zu entfernen, verwenden Sie die **--setaltmulticast** Option des **ccs** Befehls, geben aber keine Multicast-Adresse an. Beachten Sie, dass dieser Befehl alle anderen Eigenschaften, die Sie mit der **--setmulticast** Option erstellen können, auf die Standardwerte zurücksetzt, wie in Abschnitt 5.1.5, „Befehle, die vorhergehende Einstellungen überschreiben“ beschrieben.

Wenn Sie die Konfiguration aller Komponenten Ihres Clusters abgeschlossen haben, müssen Sie die Cluster-Konfigurationsdatei auf allen Knoten synchronisieren, wie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“ beschrieben.

5.15. Verbreiten der Konfigurationsdatei auf den Cluster-Knoten

Nachdem Sie auf einem der Knoten im Cluster eine Cluster-Konfigurationsdatei erstellt oder bearbeitet haben, müssen Sie diese Datei auf alle Cluster-Knoten verbreiten und die Konfiguration aktivieren.

Verwenden Sie den folgenden Befehl, um eine Cluster-Konfigurationsdatei zu verbreiten und zu aktivieren:

```
ccs -h host --sync --activate
```

Um zu überprüfen, ob alle in der Cluster-Konfigurationsdatei des Hosts spezifizierten Knoten über

identische Cluster-Konfigurationsdateien verfügen, führen Sie den folgenden Befehl aus:

```
ccs -h host --checkconf
```

Falls Sie auf einem lokalen Knoten eine Cluster-Konfigurationsdatei erstellt oder bearbeitet haben, verwenden Sie den folgenden Befehl, um diese Datei an einen der Knoten im Cluster zu übertragen:

```
ccs -f file -h host --setconf
```

Um zu überprüfen, ob alle in der lokalen Datei spezifizierten Knoten über identische Cluster-Konfigurationsdateien verfügen, führen Sie den folgenden Befehl aus:

```
ccs -f file --checkconf
```

Kapitel 6. Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit ccs

Dieses Kapitel erläutert die verschiedenen administrativen Aufgaben zur Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mithilfe des **ccs** Befehls, der ab der Red Hat Enterprise Linux 6.1 Release unterstützt wird. Dieses Kapitel umfasst die folgenden Abschnitte:

- Abschnitt 6.1, „Verwaltung von Cluster-Knoten“
- Abschnitt 6.2, „Starten und Stoppen eines Clusters“
- Abschnitt 6.3, „Fehlerdiagnose und -behebung in einem Cluster“

6.1. Verwaltung von Cluster-Knoten

Dieser Abschnitt beschreibt, wie die folgenden Features zur Knotenverwaltung mithilfe des **ccs** Befehls durchgeführt werden:

- Abschnitt 6.1.1, „Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen“
- Abschnitt 6.1.2, „Ein Mitglied zu einem laufenden Cluster hinzufügen“

6.1.1. Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen

Sie können den **ccs** Befehl dazu verwenden, um einen Knoten zum Verlassen eines Clusters zu veranlassen, indem Sie alle Cluster-Dienste auf diesem Knoten stoppen. Wenn Sie einen Knoten zum Verlassen eines Clusters veranlassen, löscht dies nicht die Cluster-Konfigurationsinformationen auf diesem Knoten. Vielmehr wird dadurch verhindert, dass dieser Knoten automatisch wieder dem Cluster beitritt, wenn dieser neu startet.

Um einen Knoten zum Verlassen eines Clusters zu veranlassen, führen Sie den folgenden Befehl aus, wodurch die Cluster-Dienste auf dem mit der **-h** Option spezifizierten Knoten beendet werden.

```
ccs -h host --stop
```

Wenn Sie Cluster-Dienste auf einem Knoten stoppen, werden Dienste, die auf diesem Knoten laufen, auf andere Knoten verlegt.

Um einen Knoten vollständig aus der Cluster-Konfiguration zu löschen, verwenden Sie die **--rmnode** Option des **ccs** Befehls, wie in Abschnitt 5.4, „Erstellen eines Clusters“ beschrieben.

Um einen Knoten zum Wiedereintritt in den Cluster zu veranlassen, führen Sie den folgenden Befehl aus, wodurch die Cluster-Dienste auf dem mit der **-h** Option spezifizierten Knoten gestartet werden.

```
ccs -h host --start
```

6.1.2. Ein Mitglied zu einem laufenden Cluster hinzufügen

Um ein Mitglied zu einem laufenden Cluster hinzuzufügen, fügen Sie dem Cluster einen Knoten wie in Abschnitt 5.4, „Erstellen eines Clusters“ beschrieben hinzu. Nachdem die Konfigurationsdatei aktualisiert wurde, verbreiten Sie diese an alle Knoten im Cluster und aktivieren Sie die neue Cluster-Konfigurationsdatei, wie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“ beschrieben.

6.2. Starten und Stoppen eines Clusters

Sie können den **ccs** Befehl dazu verwenden, um einen Cluster zu stoppen, indem Sie mithilfe des folgenden Befehls die Cluster-Dienste auf allen Knoten im Cluster stoppen:

```
ccs -h host --stopall
```

Sie können den **ccs** Befehl dazu verwenden, um einen derzeit nicht laufenden Cluster zu starten, indem Sie mithilfe des folgenden Befehls die Cluster-Dienste auf allen Knoten im Cluster starten:

```
ccs -h host --startall
```

6.3. Fehlerdiagnose und -behebung in einem Cluster

Für Informationen über die Diagnose und Behebung von Problemen in einem Cluster, siehe Kapitel 9, *Fehlerdiagnose und -behebung in einem Cluster*. Es gibt zudem einige einfache Tests, die Sie mit dem **css** Befehl vornehmen können.

Um zu überprüfen, ob alle in der Cluster-Konfigurationsdatei des Hosts spezifizierten Knoten über identische Cluster-Konfigurationsdateien verfügen, führen Sie den folgenden Befehl aus:

```
ccs -h host --checkconf
```

Falls Sie eine Konfigurationsdatei auf einem lokalen Knoten bearbeitet oder erstellt haben, können Sie überprüfen, ob alle in der lokalen Datei spezifizierten Knoten über identische Cluster-Konfigurationsdateien verfügen, indem Sie den folgenden Befehl ausführen:

```
ccs -f file --checkconf
```

Kapitel 7. Manuelle Konfiguration von Red Hat Hochverfügbarkeit

Dieses Kapitel erläutert, wie Sie die Red Hat Hochverfügbarkeits-Add-On-Software durch direktes Bearbeiten der Cluster-Konfigurationsdatei (**`/etc/cluster/cluster.conf`**) und unter Verwendung von Befehlszeilen-Tools konfigurieren können. Das Kapitel zeigt Verfahren zum abschnittsweisen Erstellen einer Konfigurationsdatei, ausgehend von einer bereitgestellten Beispieldatei. Alternativ zur Bearbeitung der hier bereitgestellten Beispieldatei können Sie auch das Gerüst für die Konfigurationsdatei von der **`cluster.conf`** Handbuchseite kopieren, allerdings lassen sich die in den nachfolgenden Verfahren angegebenen Informationen dann nicht unbedingt auf diesen Fall übertragen. Es gibt verschiedene Wege zum Erstellen und Konfigurieren einer Cluster-Konfigurationsdatei; dieses Kapitel beschreibt die Verfahren zum abschnittsweisen Erstellen einer Konfigurationsdatei. Bedenken Sie zudem, dass dieses Kapitel nur ein Ausgangspunkt zur Entwicklung einer Konfigurationsdatei sein kann und Sie Ihre Konfigurationsdatei ggf. weiter auf Ihre Clustering-Bedürfnisse anpassen müssen.

Dieses Kapitel umfasst die folgenden Abschnitte:

- Abschnitt 7.1, „Konfigurationsaufgaben“
- Abschnitt 7.2, „Erstellen einer einfachen Cluster-Konfigurationsdatei“
- Abschnitt 7.3, „Konfiguration von Fencing“
- Abschnitt 7.4, „Konfiguration von Ausfallsicherungs-Domains“
- Abschnitt 7.5, „Konfiguration von Hochverfügbarkeitsdiensten“
- Abschnitt 7.7, „Konfiguration von Debugging-Optionen“
- Abschnitt 7.6, „Konfiguration von Redundant Ring Protocol“
- Abschnitt 7.9, „Überprüfen der Konfiguration“



Wichtig

Stellen Sie sicher, dass Ihre Bereitstellung des Red Hat Hochverfügbarkeits-Add-Ons Ihren Anforderungen gerecht wird und unterstützt werden kann. Beratschlagen Sie sich dazu ggf. mit einem autorisierten Red Hat Vertreter, um Ihre Konfiguration vor der Bereitstellung zu prüfen. Berücksichtigen Sie zudem eine gewisse Zeit für einen Burn-In-Test, um die Konfiguration auf mögliche Ausfälle zu überprüfen.



Wichtig

Dieses Kapitel verweist auf häufig verwendete **`cluster.conf`** Elemente und Parameter. Eine vollständige Liste samt Beschreibung aller **`cluster.conf`** Elemente und Parameter finden Sie im Cluster-Schema unter **`/usr/share/cluster/cluster.rng`** und das kommentierte Schema unter **`/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html`** (zum Beispiel **`/usr/share/doc/cman-3.0.12/cluster_conf.html`**).



Wichtig

Bestimmte Verfahren in diesem Kapitel erfordern, dass der **`cman_tool version -r`** Befehl zum Verbreiten der Cluster-Konfiguration im gesamten Cluster ausgeführt wird. Für die Verwendung dieses Befehls ist es erforderlich, dass **`ricci`** läuft. Die Verwendung von **ricci** erfordert ein Passwort, wenn Sie zum ersten Mal von einem bestimmten Rechner aus mit **ricci** interagieren. Informationen über den **`ricci`** Dienst finden Sie in Abschnitt 2.13, „Überlegungen zu **`ricci`**“.



Anmerkung

Einige Verfahren in diesem Kapitel enthalten bestimmte Befehle für die in *Anhang E, Überblick über Befehlszeilen-Tools* aufgelisteten Befehlszeilen-Tools. Für weitere Informationen über alle Befehle und Variablen siehe die Handbuchseite des jeweiligen Befehlszeilen-Tools.

7.1. Konfigurationsaufgaben

Zur Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software mit Befehlszeilen-Tools gehören die folgenden Schritte:

1. Erstellen eines Clusters. Siehe Abschnitt 7.2, „Erstellen einer einfachen Cluster-Konfigurationsdatei“.
2. Konfiguration des Fencings. Siehe Abschnitt 7.3, „Konfiguration von Fencing“.
3. Konfiguration von Ausfallsicherungs-Domains. Siehe Abschnitt 7.4, „Konfiguration von Ausfallsicherungs-Domains“.
4. Konfiguration von Hochverfügbarkeitsdiensten. Siehe Abschnitt 7.5, „Konfiguration von Hochverfügbarkeitsdiensten“.
5. Überprüfen der Konfiguration. Siehe Abschnitt 7.9, „Überprüfen der Konfiguration“.

7.2. Erstellen einer einfachen Cluster-Konfigurationsdatei

Sofern die Cluster-Hardware, Red Hat Enterprise Linux und die Hochverfügbarkeits-Add-On-Software installiert sind, können Sie eine Cluster-Konfigurationsdatei (**/etc/cluster/cluster.conf**) erstellen und das Hochverfügbarkeits-Add-On starten. Dieser Abschnitt soll Ihnen als Ausgangspunkt dienen und beschreibt, wie Sie das Gerüst für eine Cluster-Konfigurationsdatei erstellen, allerdings noch ohne Fencing, Ausfallsicherungs-Domains oder Hochverfügbarkeitsdiensten - mit diesen Aspekten der Konfigurationsdatei befassen sich spätere Abschnitte.



Wichtig

Hierbei handelt es sich lediglich um einen Zwischenschritt zur Erstellung einer Cluster-Konfigurationsdatei; die hieraus resultierende Datei beinhaltet kein Fencing und ist keine gültige Konfiguration.

Die folgenden Schritte beschreiben die Erstellung und Konfiguration eines Gerüsts für eine Cluster-Konfigurationsdatei. Letztendlich unterscheidet sich die Konfigurationsdatei für Ihren Cluster abhängig von der Anzahl der Knoten, vom Fencing-Typ, von der Anzahl und der Art der Hochverfügbarkeitsdienste sowie von weiteren umgebungsspezifischen Anforderungen.

1. Erstellen Sie auf jedem Knoten im Cluster eine **/etc/cluster/cluster.conf** Datei. Verwenden Sie dazu die Vorlage in Beispiel 7.1, „**cluster.conf** Beispiel: Grundlegende Konfiguration“.
2. **(Optional)** Falls Sie einen Zwei-Knoten-Cluster ausführen, können Sie die folgende Zeile zur Konfigurationsdatei hinzufügen, damit es einem einzelnen Knoten möglich ist, das Quorum zu erhalten (z.B. falls der andere Knoten ausfällt):

   ```
   <cman two_node="1" expected_votes="1"/>
   ```

   Wenn Sie die **two_node** Option aus der **cluster.conf** Datei entfernen oder ihr hinzufügen, so müssen Sie den Cluster neu starten, damit diese Änderung wirksam wird, wenn Sie die Konfiguration aktualisieren. Für Informationen über das Aktualisieren einer Cluster-Konfiguration siehe Abschnitt 8.4, „Aktualisieren einer Konfiguration“. Ein Beispiel für das Spezifizieren der **two_node** Option finden Sie in Beispiel 7.2, „**cluster.conf** Beispiel: Einfache Zwei-Knoten-

Konfiguration“.

3. Geben Sie den Cluster-Namen und die Versionsnummer der Konfiguration mithilfe dieser **cluster** Parameter an: **name** und **config_version** (siehe Beispiel 7.1, „**cluster.conf** Beispiel: Grundlegende Konfiguration“ oder Beispiel 7.2, „**cluster.conf** Beispiel: Einfache Zwei-Knoten-Konfiguration“).
4. Geben Sie im **clusternodes** Abschnitt den Knotennamen und die Knoten-ID eines jeden Knotens mithilfe dieser **clusternode** Parameter an: **name** und **nodeid**. Der Knotenname darf maximal 255 Bytes lang sein.
5. Speichern Sie die **/etc/cluster/cluster.conf** ab.
6. Überprüfen Sie die Datei anhand des Cluster-Schemas (**cluster.rng**), indem Sie den **ccs_config_validate** Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Übertragen Sie die Konfigurationsdatei nach **/etc/cluster/** in jedem Cluster-Knoten. Beispielsweise könnten Sie die Datei mithilfe des **scp** Befehls an andere Cluster-Knoten übertragen.



Anmerkung

Eine solche Übertragung der Cluster-Konfigurationsdatei ist nur beim erstmaligen Erstellen des Clusters notwendig. Sobald ein Cluster installiert wurde und läuft, kann die Cluster-Konfigurationsdatei mit dem Befehl **cman_tool version -r** übertragen werden. Es ist möglich, den **scp** Befehl zur Weitergabe einer aktualisierten Konfigurationsdatei zu verwenden, allerdings muss zur Verwendung des **scp** Befehls auf allen Knoten die Cluster-Software gestoppt werden. Zusätzlich sollten Sie **ccs_config_validate** ausführen, falls Sie eine aktualisierte Konfigurationsdatei mittels **scp** übertragen.



Anmerkung

Es sind zwar noch andere Elemente und Parameter in der Beispielkonfigurationsdatei enthalten (z.B. **fence** und **fencedevices**), vorerst ist es jedoch nicht nötig, diese mit Informationen auszufüllen. An späterer Stelle in diesem Kapitel werden Verfahren erläutert, die Informationen zu diesen Elementen und Parametern liefern.

8. Starten Sie den Cluster. Führen Sie dazu auf jedem Cluster-Knoten den folgenden Befehl aus:

   service cman start

   Zum Beispiel:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
```

9. Führen Sie auf einem beliebigen Cluster-Knoten **`cman_tool nodes`** aus, um zu überprüfen, dass die Knoten nun als Mitglieder im Cluster fungieren (gekennzeichnet durch ein "M" in der Statusspalte "Sts"). Zum Beispiel:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
   3   M    544   2010-09-28 10:52:21  node-03.example.com
```

10. Läuft der Cluster, fahren Sie mit Abschnitt 7.3, „Konfiguration von Fencing“ fort.

Einfache Konfigurationsbeispiele

Beispiel 7.1, „`cluster.conf` Beispiel: Grundlegende Konfiguration“ und Beispiel 7.2, „`cluster.conf` Beispiel: Einfache Zwei-Knoten-Konfiguration“ (bei einem Zwei-Knoten-Cluster) liefern jeweils eine sehr einfache Beispiel-Cluster-Konfigurationsdatei als Ausgangspunkt. An späterer Stelle in diesem Kapitel werden Verfahren erläutert, die Informationen über die Konfiguration von Fencing und Hochverfügbarkeitsdiensten liefern.

Beispiel 7.1. `cluster.conf` Beispiel: Grundlegende Konfiguration

```
<cluster name="mycluster" config_version="2">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Beispiel 7.2. `cluster.conf` Beispiel: Einfache Zwei-Knoten-Konfiguration

```
<cluster name="mycluster" config_version="2">
   <cman two_node="1" expected_votes="1"/>
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Der consensus Wert für `totem` in einen Zwei-Knoten-Cluster

Wenn Sie einen Zwei-Knoten-Cluster erstellen und nicht beabsichtigen, diesem zu einem späteren Zeitpunkt weitere Knoten hinzuzufügen, dann sollten Sie den **consensus** Wert im **`totem`** Tag in der **`cluster.conf`** Datei weglassen, so dass der **consensus** Wert automatisch ermittelt wird. Beim automatischen Ermitteln des **consensus** Wertes gelten die folgenden Regeln:

- Bei zwei oder weniger Knoten lautet der **consensus** Wert (Token * 0.2), mit einer Höchstgrenze von 2000 ms und einer Mindestgrenze von 200 ms.
- Bei drei oder mehr Knoten lautet der **consensus** Wert (Token + 2000 ms)

Wenn Sie das **`cman`** Dienstprogramm Ihren Consensus-Timeout auf diese Weise bestimmen lassen, müssen Sie später, falls Sie von zwei auf drei oder mehr Knoten aufstocken, Ihren Cluster neu starten, da der Consensus-Timeout dann auf den höheren Wert geändert werden muss, entsprechend dem Token-Timeout.

Wenn Sie einen Zwei-Knoten-Cluster konfigurieren und beabsichtigen, diesen zukünftig auf mehr als zwei Knoten zu erweitern, können Sie den Consensus-Timeout außer Kraft setzen, so dass ein Cluster-Neustart nicht nötig ist, wenn Sie von zwei auf drei oder mehr Knoten aufstocken. Bearbeiten Sie dazu die **`cluster.conf`** wie folgt:

```
<totem token="X" consensus="X + 2000" />
```

Beachten Sie, dass bei der Verarbeitung der Konfiguration X + 2000 nicht automatisch berechnet wird. Sie müssen daher einen ganzzahligen Wert einsetzen, keine Formel.

Der Vorteil bei der Verwendung des optimierten Consensus-Timeouts für Zwei-Knoten-Cluster besteht darin, dass die Zeit beim Knotenwechsel im Fehlerfall reduziert wird, da Consensus keine Funktion des Token-Timeouts ist.

Beachten Sie, dass für die automatische Zwei-Knoten-Erkennung in **`cman`** die Anzahl der physischen Knoten maßgeblich ist, nicht das Vorhandensein der **`two_node=1`** Direktive in der **`cluster.conf`** Datei.

7.3. Konfiguration von Fencing

Zur Konfiguration von Fencing gehört (a) das Angeben eines oder mehrerer Fencing-Geräte in einem Cluster und (b) das Angeben einer oder mehrerer Fencing-Methoden für jeden Knoten (unter Verwendung der angegebenen Fencing-Geräte).



Anmerkung

Es wird empfohlen, für jeden Knoten mehrere Fencing-Mechanismen zu konfigurieren. Ein Fencing-Gerät kann aus verschiedenen Gründen ausfallen, beispielsweise aufgrund einer Netzwerkspaltung, eines Stromausfalls oder eines Problems mit dem Fencing-Gerät selbst. Die Konfiguration mehrerer Fencing-Mechanismen verringert die Wahrscheinlichkeit, dass der Ausfall eines Fencing-Geräts schwerwiegende Folgen hat.

Konfigurieren Sie abhängig von den Fencing-Gerätetypen und den Fencing-Methoden, die für Ihre Konfiguration notwendig sind, die **cluster.conf** folgendermaßen:

1. Geben Sie im **fencedevices** Abschnitt jedes Fencing-Geräts mittels eines **fencedevice** Elements und den von dem Fencing-Gerät abhängigen Parametern an. Beispiel 7.3, „APC Fencing-Gerät zu **cluster.conf** hinzugefügt“ zeigt ein Beispiel für eine Konfigurationsdatei, zu der ein APC-Fencing-Gerät hinzugefügt wurde.
2. Geben Sie im **clusternodes** Abschnitt innerhalb des **fence** Elements für jeden **clusternode** Abschnitt die Fencing-Methode für den Knoten an. Spezifizieren Sie den Fencing-Methodennamen mithilfe des **method** Parameters **name**. Geben Sie das Fencing-Gerät für jede Fencing-Methode an, und zwar mithilfe des **device** Elements und dessen Parametern, **name** und Fencing-Gerät-spezifischen Parametern. Beispiel 7.4, „Fencing-Methoden zu **cluster.conf** hinzugefügt“ zeigt ein Beispiel für eine Fencing-Methode mit einem Fencing-Gerät für jeden Knoten im Cluster.
3. Fügen Sie für andere Fencing-Methoden als das Power-Fencing (also SAN/Speicher-Fencing) im **clusternodes** Abschnitt einen **unfence** Abschnitt ein. Dadurch wird sichergestellt, dass ein abgegrenzter Knoten erst wieder re-aktiviert wird, nachdem er neu gestartet wurde. Wenn Sie ein Gerät konfigurieren, dass Unfencing erfordert, muss der Cluster zunächst gestoppt werden, dann muss die vollständige Konfiguration einschließlich Geräten und Unfencing hinzugefügt werden, bevor der Cluster gestartet wird. Weitere Informationen über das Aufheben der Knotenabgrenzung finden Sie auf der **fence_node**(8) Handbuchseite.

   Der **unfence** Abschnitt enthält im Gegensatz zum **fence** Abschnitt keine **method** Abschnitte. Er enthält direkte **device** Referenzen, welche die entsprechenden Geräteabschnitte für **fence** widerspiegeln, sowie zusätzlich die explizite Aktion (**action**) "on" oder "enable". Dasselbe **fencedevice** wird sowohl von den **fence** als auch von **unfence device** Zeilen referenziert, und es sollten dieselben Parameter für den Knoten wiederholt werden.

   Indem Sie den **action** Parameter auf "on" oder "enable" setzen, wird dieser Knoten nach einem Neustart aktiviert. Beispiel 7.4, „Fencing-Methoden zu **cluster.conf** hinzugefügt“ und Beispiel 7.5, „**cluster.conf**: Mehrere Fencing-Methoden pro Knoten“ enthalten Beispiele für die **unfence** Elemente und Parameter.

   Für weitere Informationen über **unfence** werfen Sie einen Blick auf die **fence_node** Handbuchseite.
4. Aktualisieren Sie den **config_version** Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von **config_version="2"** auf **config_version="3"**).
5. Speichern Sie die **/etc/cluster/cluster.conf** ab.
6. **(Optional)** Überprüfen Sie die aktualisierte Datei anhand des Cluster-Schemas (**cluster.rng**), indem Sie den **ccs_config_validate** Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Führen Sie den **cman_tool version -r** Befehl aus, um die Konfiguration an die übrigen Cluster-Knoten zu verbreiten. Dadurch wird auch eine zusätzliche Validierung ausgeführt. Es ist notwendig, dass **ricci** auf jedem Cluster-Knoten ausgeführt wird, um die aktualisierten Cluster Konfigurationsdaten verbreiten zu können.
8. Vergewissern Sie sich, dass die aktualisierte Konfigurationsdatei übertragen wurde.
9. Fahren Sie mit Abschnitt 7.4, „Konfiguration von Ausfallsicherungs-Domains“ fort.

Falls nötig, können Sie komplexe Konfigurationen mit mehreren Fencing-Methoden pro Knoten und mit mehreren Fencing-Geräten pro Methode konfigurieren. Falls mehrere Fencing-Methoden pro Knoten konfiguriert sind und die Abgrenzung mit der ersten Methode fehlschlägt, versucht der Fencing-Daemon **fenced** die nächste Methode usw., bis er schließlich eine Methode findet, die funktioniert.

Manchmal ist es zur Abgrenzung eines Knotens nötig, zwei I/O-Pfade oder zwei Stromversorgungen zu deaktivieren. Sie erreichen dies durch Angabe von zwei (oder mehr) Geräten innerhalb der Fencing-Methode. **fenced** führt den Fenching-Agent einmal für jede Fencing-Gerätezeile aus; alle müssen erfolgreich verlaufen, damit das Fencing insgesamt erfolgreich ist.

Komplexere Konfigurationen werden im Abschnitt „Fencing-Konfigurationsbeispiele“ veranschaulicht.

Weitere Informationen über die Konfiguration bestimmter Fencing-Geräte finden Sie auf der Handbuchseite eines Fencing-Geräte-Agenten (z.B. auf der Handbuchseite für **fence_apc**). Des Weiteren finden Sie Informationen über Fencing-Parameter in Anhang A, *Parameter der Fencing-Geräte*, den Fencing-Agenten in **/usr/sbin/**, das Cluster-Schema unter **/usr/share/cluster/cluster.rng**, und das kommentierte Schema unter **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (z.B. **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

Fencing-Konfigurationsbeispiele

Das folgende Beispiel zeigt eine einfache Konfiguration mit einer Fencing-Methode pro Knoten und einem Fencing-Gerät pro Fencing-Methode:

- Beispiel 7.3, „APC Fencing-Gerät zu **cluster.conf** hinzugefügt“
- Beispiel 7.4, „Fencing-Methoden zu **cluster.conf** hinzugefügt“

Die folgenden Beispiele zeigen komplexere Konfigurationen:

- Beispiel 7.5, „**cluster.conf**: Mehrere Fencing-Methoden pro Knoten“
- Beispiel 7.6, „**cluster.conf**: Fencing, Multi-Pathing mehrerer Ports“
- Beispiel 7.7, „**cluster.conf**: Fencing von Knoten mit Dual-Stromversorgung“



Anmerkung

Die Beispiele in diesem Abschnitt können nicht alle möglichen Fälle aufzeigen, es gibt also durchaus andere Wege, wie Sie das Fencing Ihren Anforderungen entsprechend konfigurieren können.

Beispiel 7.3. APC Fencing-Gerät zu `cluster.conf` hinzugefügt

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

In diesem Beispiel wurde ein Fencing-Gerät (**`fencedevice`**) zum **`fencedevices`** Element hinzugefügt und spezifiziert den Fencing-Agenten (**`agent`**) als **`fence_apc`**, die IP-Adresse (**`ipaddr`**) als **`apc_ip_example`**, das Login (**`login`**) als **`login_example`**, den Namen des Fencing-Geräts (**`name`**) als **`apc`** und das Passwort (**`passwd`**) als **`password_example`**.

Beispiel 7.4. Fencing-Methoden zu `cluster.conf` hinzugefügt

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

In diesem Beispiel wurde eine Fencing-Methode (**`method`**) zu jedem Knoten hinzugefügt. Der Name der Fencing-Methode (**`name`**) für jeden Knoten ist **`APC`**. Das Gerät (**`device`**) für die Fencing-Methode in jedem Knoten spezifiziert den Namen (**`name`**) als **`apc`** und eine eindeutige APC Switch Netzanschlussnummer (**`port`**) für jeden Knoten. Zum Beispiel lautet die Netzanschlussnummer für node-01.example.com **`1`** (**`port="1"`**). Der Gerätename für jeden Knoten (**`device name="apc"`**) verweist auf das Fencing-Gerät anhand des Namens (**`name`**) **`apc`** in dieser Zeile des **`fencedevices`** Elements: **`fencedevice agent="fence_apc" ipaddr="apc_ip_example" login="login_example" name="apc" passwd="password_example"`**.

Beispiel 7.5. `cluster.conf`: Mehrere Fencing-Methoden pro Knoten

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
            <method name="SAN">
       <device name="sanswitch1" port="11"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="11" action="on"/>
         </unfence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
            <method name="SAN">
       <device name="sanswitch1" port="12"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="12" action="on"/>
         </unfence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
            <method name="SAN">
       <device name="sanswitch1" port="13"/>
             </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="13" action="on"/>
         </unfence>
     </clusternode>
   </clusternodes>
   <fencedevices>
        <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
        <fencedevice agent="fence_sanbox2" ipaddr="san_ip_example"
login="login_example" name="sanswitch1" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Beispiel 7.6. `cluster.conf`: Fencing, Multi-Pathing mehrerer Ports

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="SAN-multi">
       <device name="sanswitch1" port="11"/>
       <device name="sanswitch2" port="11"/>
     </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="11" action="on"/>
             <device name="sanswitch2" port="11" action="on"/>
         </unfence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="SAN-multi">
       <device name="sanswitch1" port="12"/>
       <device name="sanswitch2" port="12"/>
            </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="12" action="on"/>
             <device name="sanswitch2" port="12" action="on"/>
         </unfence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="SAN-multi">
       <device name="sanswitch1" port="13"/>
       <device name="sanswitch2" port="13"/>
            </method>
         </fence>
         <unfence>
             <device name="sanswitch1" port="13" action="on"/>
             <device name="sanswitch2" port="13" action="on"/>
         </unfence>
     </clusternode>
   </clusternodes>
   <fencedevices>
        <fencedevice agent="fence_sanbox2" ipaddr="san_ip_example"
login="login_example" name="sanswitch1" passwd="password_example"/>
        <fencedevice agent="fence_sanbox2" ipaddr="san_ip_example"
login="login_example" name="sanswitch2" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Beispiel 7.7. `cluster.conf`: Fencing von Knoten mit Dual-Stromversorgung

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC-dual">
              <device name="apc1" port="1"action="off"/>
              <device name="apc2" port="1"action="off"/>
              <device name="apc1" port="1"action="on"/>
              <device name="apc2" port="1"action="on"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC-dual">
              <device name="apc1" port="2"action="off"/>
              <device name="apc2" port="2"action="off"/>
              <device name="apc1" port="2"action="on"/>
              <device name="apc2" port="2"action="on"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC-dual">
              <device name="apc1" port="3"action="off"/>
              <device name="apc2" port="3"action="off"/>
              <device name="apc1" port="3"action="on"/>
              <device name="apc2" port="3"action="on"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
       <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc1" passwd="password_example"/>
       <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc2" passwd="password_example"/>
   </fencedevices>
   <rm>
   </rm>
</cluster>
```

Werden Netzschalter zum Abgrenzen von Knoten mit dualer Stromversorgung verwendet, muss den Agenten mitgeteilt werden, beide Netzanschlüsse zu deaktivieren, bevor die Stromversorgung auf einem der beiden Anschlüsse wiederhergestellt werden kann. Das standardmäßige Verhalten des Agenten beim ein- und ausschalten könnte andernfalls dazu führen, dass die Stromversorgung auf dem Knoten nie vollständig abgeschaltet wird.

7.4. Konfiguration von Ausfallsicherungs-Domains

Eine Ausfallsicherungs-Domain ist eine benannte Teilmenge von Cluster-Knoten, die dazu berechtigt ist, einen Cluster-Dienst im Falle eines Knotenausfalls weiterzuführen. Eine Ausfallsicherungs-Domain kann die folgenden Charakteristiken haben:

- Uneingeschränkt — Ermöglicht Ihnen, eine Teilmenge bevorzugter Mitglieder zu spezifizieren, doch der dieser Domain zugewiesene Cluster-Dienst kann auf jedem verfügbaren Mitglied ausgeführt werden.
- Eingeschränkt — Ermöglicht Ihnen, die Mitglieder einzuschränken, auf denen ein bestimmter Cluster-Dienst laufen darf. Falls keines der Mitglieder in einer eingeschränkten Ausfallsicherungs-Domain verfügbar ist, kann der Cluster-Dienst nicht gestartet werden (weder manuell noch durch die Cluster-Software).
- Ungeordnet — Wenn ein Cluster-Dienst einer ungeordneten Aufallsicherungs-Domain zugewiesen ist, wird das Mitglied, auf dem der Cluster-Dienst ausgeführt wird, ohne Berücksichtigung von Prioritäten aus den verfügbaren Mitgliedern der Ausfallsicherungs-Domain ausgewählt.
- Geordnet — Ermöglicht Ihnen, eine Prioritätsreihenfolge für die Mitglieder einer Ausfallsicherungs-Domain anzugeben. Geordnete Ausfallsicherungs-Domains wählen den Knoten mit der niedrigsten Priorität zuerst. Das heißt, dass der Knoten in der Ausfallsicherungs-Domain mit der Priorität "1" die höchste Priorität hat und demnach der bevorzugte Knoten in einer Ausfallsicherungs-Domain ist. Der nächste bevorzugte Knoten wäre also der Knoten mit der nächsthöheren Priorität, usw.
- Failback — Ermöglicht Ihnen festzulegen, ob ein Dienst in der Ausfallsicherungs-Domain auf den Knoten zurückwechseln soll, auf dem er vor dessen Ausfall ursprünglich ausgeführt wurde. Das Konfigurieren dieser Charakteristik ist hilfreich in Situationen, in denen ein Knoten häufig ausfällt und Teil einer geordneten Ausfallsicherungs-Domain ist. In diesem Fall würde ein Dienst, der auf dem bevorzugten Knoten in einer Ausfallsicherungs-Domain läuft, möglicherweise wiederholt zwischen dem bevorzugten Knoten und einem anderen Knoten hin- und her wechseln, was beträchtliche Leistungseinbußen zur Folge hätte.

  Anmerkung

  Die Failback-Charakteristik greift nur, wenn die geordnete Ausfallsicherung konfiguriert ist.



Anmerkung

Eine Änderung der Ausfallsicherungs-Domain-Konfiguration hat keine Auswirkungen auf derzeit laufende Dienste.



Anmerkung

Ausfallsicherungs-Domains werden für den Betrieb *nicht* benötigt.

Standardmäßig sind Ausfallsicherungs-Domains uneingeschränkt und ungeordnet.

In einem Cluster mit mehreren Mitgliedern kann Ihnen der Einsatz einer beschränkten Ausfallsicherungs-Domain die Arbeit erleichtern. Denn um einen Cluster zum Ausführen eines Cluster-Dienstes (wie z.B. **`httpd`**) einzurichten, müssen Sie auf allen Cluster-Mitgliedern, die diesen Cluster-Dienst ausführen sollen, eine identische Konfiguration einrichten. Anstatt den gesamten Cluster zur Ausführung dieses Cluster-Dienstes einzurichten, müssen Sie somit nur die Mitglieder der beschränkten Ausfallsicherungs-Domain, die Sie mit diesem Cluster-Dienst verknüpfen möchten, entsprechend einrichten.



Anmerkung

Um ein bevorzugtes Mitglied zu konfigurieren, können Sie eine uneingeschränkte Ausfallsicherungs-Domain einrichten, die nur aus einem Cluster-Mitglied besteht. Dadurch läuft der Cluster-Dienst zwar hauptsächlich auf diesem einen Cluster-Mitglied (dem bevorzugten Mitglied), doch erlaubt es dem Cluster-Dienst gleichzeitig, im Falle eines Ausfalls auf einen beliebigen anderen Knoten zu wechseln.

Gehen Sie folgendermaßen vor, um eine Ausfallsicherungs-Domain zu konfigurieren:

1. Öffnen Sie **/etc/cluster/cluster.conf** auf einem beliebigen Knoten im Cluster.
2. Fügen Sie das folgende Gerüst innerhalb des **rm** Elements für jede zu verwendende Ausfallsicherungs-Domain hinzu:

```
        <failoverdomains>
            <failoverdomain name="" nofailback="" ordered="" restricted="">
                <failoverdomainnode name="" priority=""/>
                <failoverdomainnode name="" priority=""/>
                <failoverdomainnode name="" priority=""/>
            </failoverdomain>
        </failoverdomains>
```



Anmerkung

Die Anzahl der **failoverdomainnode** Parameter hängt von der Anzahl der Knoten in der Ausfallsicherungs-Domain ab. Das oben gezeigte Gerüst für den **failoverdomain** Abschnitt enthält drei **failoverdomainnode** Elemente (ohne spezifizierte Knotennamen), was bedeutet, dass es drei Knoten in der Ausfallsicherungs-Domain gibt.

3. Geben Sie im **failoverdomain** Abschnitt die Werte für die Elemente und Parameter an. Beschreibungen der Elemente und Parameter finden Sie im *failoverdomain* Abschnitt des kommentierten Cluster-Schemas. Das kommentierte Cluster-Schema ist in jedem Cluster-Knoten verfügbar unter **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (z.B. **/usr/share/doc/cman-3.0.12/cluster_conf.html**). Ein Beispiel für einen **failoverdomains** Abschnitt finden Sie in Beispiel 7.8, „Eine Ausfallsicherungs-Domain zu **cluster.conf** hinzugefügt“.
4. Aktualisieren Sie den **config_version** Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von **config_version="2"** auf **config_version="3"**).
5. Speichern Sie die **/etc/cluster/cluster.conf** ab.
6. **(Optional)** Überprüfen Sie die Datei anhand des Cluster-Schemas (**cluster.rng**), indem Sie den **ccs_config_validate** Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Führen Sie den **cman_tool version -r** Befehl durch, um die Konfiguration an die übrigen Cluster-Knoten weiterzugeben.
8. Fahren Sie mit Abschnitt 7.5, „Konfiguration von Hochverfügbarkeitsdiensten“ fort.

Beispiel 7.8, „Eine Ausfallsicherungs-Domain zu **cluster.conf** hinzugefügt“ zeigt ein Beispiel für eine Konfiguration mit einer geordneten, uneingeschränkten Ausfallsicherungs-Domain.

Beispiel 7.8. Eine Ausfallsicherungs-Domain zu `cluster.conf` hinzugefügt

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
       <failoverdomains>
           <failoverdomain name="example_pri" nofailback="0" ordered="1"
restricted="0">
               <failoverdomainnode name="node-01.example.com" priority="1"/>
               <failoverdomainnode name="node-02.example.com" priority="2"/>
               <failoverdomainnode name="node-03.example.com" priority="3"/>
           </failoverdomain>
       </failoverdomains>
   </rm>
</cluster>
```

Der **`failoverdomains`** Abschnitt enthält einen **`failoverdomain`** Abschnitt für jede Ausfallsicherungs-Domain im Cluster. Dieses Beispiel hat eine Ausfallsicherungs-Domain. In der **`failoverdomain`** Zeile ist der Name (**`name`**) als **`example_pri`** spezifiziert. Zusätzlich wird kein Failback (**`failback="0"`**), eine geordnete Ausfallsicherung (**`ordered="1"`**) und die Ausfallsicherungs-Domain als uneingeschränkt (**`restricted="0"`**) spezifiziert.

7.5. Konfiguration von Hochverfügbarkeitsdiensten

Die Konfiguration von Hochverfügbarkeitsdiensten umfasst das Konfigurieren von Ressourcen und das Zuweisen derselben zu Diensten.

Die folgenden Abschnitte beschreiben, wie Sie **`/etc/cluster/cluster.conf`** zum Hinzufügen von Ressourcen und Diensten konfigurieren.

- Abschnitt 7.5.1, „Hinzufügen von Cluster-Ressourcen“

- Abschnitt 7.5.2, „Hinzufügen eines Cluster-Dienstes zum Cluster“



Wichtig

Es gibt eine Vielzahl möglicher Konfigurationen für die Hochverfügbarkeitsressourcen und -dienste. Für ein besseres Verständnis von Ressourcenparametern und Ressourcenverhalten siehe Anhang B, *Parameter der Hochverfügbarkeitsressourcen* and Anhang C, *Verhalten der Hochverfügbarkeitsressourcen*. Um optimale Leistung zu erreichen und um sicherzustellen, dass Ihre Konfiguration unterstützt werden kann, setzen Sie sich bitte mit einem autorisierten Red Hat Vertreter in Verbindung.

7.5.1. Hinzufügen von Cluster-Ressourcen

Sie können zwei Arten von Ressourcen konfigurieren:

- Global — Ressourcen, die für jeden Dienst im Cluster zur Verfügung stehen. Diese werden im **resources** Abschnitt der Konfigurationsdatei konfiguriert (innerhalb des **rm** Elements).
- Dienstspezifisch — Ressourcen, die nur für einen einzigen Dienst zur Verfügung stehen. Diese werden im jeweiligen **service** Abschnitt der Konfigurationsdatei konfiguriert (innerhalb des **rm** Elements).

Dieser Abschnitt beschreibt, wie globale Ressourcen hinzugefügt werden. Verfahren zum Konfigurieren von dienstspezifischen Ressourcen finden Sie in Abschnitt 7.5.2, „Hinzufügen eines Cluster-Dienstes zum Cluster“.

Um eine globale Cluster-Ressource hinzuzufügen, folgen Sie den Schritten in diesem Abschnitt.

1. Öffnen Sie **/etc/cluster/cluster.conf** auf einem beliebigen Knoten im Cluster.
2. Fügen Sie einen **resources** Abschnitt innerhalb des **rm** Elements hinzu. Zum Beispiel:

```
    <rm>
        <resources>

        </resources>
    </rm>
```

3. Füllen Sie es mit Ressourcen abhängig von den Diensten, die Sie erstellen möchten, aus. Sehen Sie nachfolgend beispielsweise die Ressourcen, die in einem Apache-Dienst verwendet werden. Dazu gehören eine Dateisystem-Ressource (**fs**), eine IP-Ressource (**ip**) und eine Apache-Ressource (**apache**).

```
    <rm>
        <resources>
           <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
           <ip address="127.143.131.100" monitor_link="yes" sleeptime="10"/>
           <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
        </resources>
    </rm>
```

Beispiel 7.9, „**cluster.conf** Datei mit hinzugefügten Ressourcen“ zeigt ein Beispiel einer **cluster.conf** Datei mit hinzugefügtem **resources** Abschnitt.

4. Aktualisieren Sie den **config_version** Parameter, indem Sie dessen Wert erhöhen (ändern Sie

ihn z.B. von **config_version="2"** auf **config_version="3"**).

5. Speichern Sie die **/etc/cluster/cluster.conf** ab.
6. **(Optional)** Überprüfen Sie die Datei anhand des Cluster-Schemas (**cluster.rng**), indem Sie den **ccs_config_validate** Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Führen Sie den **cman_tool version -r** Befehl durch, um die Konfiguration an die übrigen Cluster-Knoten weiterzugeben.
8. Vergewissern Sie sich, dass die aktualisierte Konfigurationsdatei übertragen wurde.
9. Fahren Sie mit Abschnitt 7.5.2, „Hinzufügen eines Cluster-Dienstes zum Cluster“ fort.

Beispiel 7.9. `cluster.conf` Datei mit hinzugefügten Ressourcen

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
       <failoverdomains>
           <failoverdomain name="example_pri" nofailback="0" ordered="1"
restricted="0">
               <failoverdomainnode name="node-01.example.com" priority="1"/>
               <failoverdomainnode name="node-02.example.com" priority="2"/>
               <failoverdomainnode name="node-03.example.com" priority="3"/>
           </failoverdomain>
       </failoverdomains>
       <resources>
           <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
           <ip address="127.143.131.100" monitor_link="yes" sleeptime="10"/>
           <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
        </resources>

   </rm>
</cluster>
```

7.5.2. Hinzufügen eines Cluster-Dienstes zum Cluster

Um einen Cluster-Dienst zum Cluster hinzuzufügen, folgen Sie den Schritten in diesem Abschnitt.



Anmerkung

Die Beispiele in diesem Abschnitt zeigen einen Cluster-Dienst, in dem sich alle Ressourcen auf derselben Ebene befinden. Werfen Sie einen Blick auf Anhang C, *Verhalten der Hochverfügbarkeitsressourcen* für Informationen über das Definieren eines Dienstes, in dem es eine Abhängigkeitenkette in der Ressourcenhierarchie gibt sowie Regeln, die das Verhalten der Eltern- und Kind-Ressourcen steuern.

1. Öffnen Sie **`/etc/cluster/cluster.conf`** auf einem beliebigen Knoten im Cluster.
2. Fügen Sie für jeden Dienst einen **`service`** Abschnitt innerhalb des **`rm`** Elements hinzu. Zum Beispiel:

```
    <rm>
        <service autostart="1" domain="" exclusive="0" name=""
recovery="restart">

        </service>
    </rm>
```

3. Konfigurieren Sie die folgenden Parameter im **`service`** Element:
   - **`autostart`** — Legt fest, ob der Dienst beim Start des Clusters automatisch gestartet werden soll. Verwenden Sie '1' zur Aktivierung und '0' zur Deaktivierung; der Standard ist aktiviert.
   - **`domain`** — Legt eine Ausfallsicherungs-Domain fest (falls erforderlich).
   - **`exclusive`** — Legt eine Richtlinie fest, gemäß der dieser Dienst ausschließlich auf Knoten ausgeführt werden darf, auf denen kein anderer Dienst läuft.
   - **`recovery`** — Legt eine Richtlinie zur Wiederherstellung des Dienstes fest. Die Optionen sind relocate, restart, disable oder restart-disable.
4. Abhängig von der Art der Ressource, die Sie verwenden möchten, füllen Sie den Dienst mit globalen oder dienstspezifischen Ressourcen aus.

   Sehen Sie hier beispielsweise einen Apache-Dienst, der globale Ressourcen verwendet:

```
    <rm>
        <resources>
                <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
                <ip address="127.143.131.100" monitor_link="yes"
sleeptime="10"/>
                <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
        </resources>
        <service autostart="1" domain="example_pri" exclusive="0"
name="example_apache" recovery="relocate">
                <fs ref="web_fs"/>
                <ip ref="127.143.131.100"/>
                <apache ref="example_server"/>
        </service>
    </rm>
```

   Und sehen Sie hier beispielsweise einen Apache-Dienst, der dienstspezifische Ressourcen verwendet:

```
    <rm>
        <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache2" recovery="relocate">
                <fs name="web_fs2" device="/dev/sdd3" mountpoint="/var/www2"
fstype="ext3"/>
                <ip address="127.143.131.101" monitor_link="yes"
sleeptime="10"/>
                <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
        </service>
    </rm>
```

Beispiel 7.10, „**cluster.conf** mit hinzugefügten Diensten: Einer verwendet globale Ressourcen, der andere verwendet dienstspezifische Ressourcen“ zeigt ein Beispiel einer **cluster.conf** Datei mit zwei Diensten:

- **example_apache** — Dieser Dienst verwendet die globalen Ressourcen **web_fs**, **127.143.131.100** und **example_server**.
- **example_apache2** — Dieser Dienst verwendet die dienstspezifischen Ressourcen **web_fs2**, **127.143.131.101** und **example_server2**.

5. Aktualisieren Sie den **config_version** Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von **config_version="2"** auf **config_version="3"**).
6. Speichern Sie die **/etc/cluster/cluster.conf** ab.
7. **(Optional)** Überprüfen Sie die aktualisierte Datei anhand des Cluster-Schemas (**cluster.rng**), indem Sie den **ccs_config_validate** Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

8. Führen Sie den **cman_tool version -r** Befehl durch, um die Konfiguration an die übrigen Cluster-Knoten weiterzugeben.
9. Vergewissern Sie sich, dass die aktualisierte Konfigurationsdatei übertragen wurde.
10. Fahren Sie mit Abschnitt 7.9, „Überprüfen der Konfiguration“ fort.

Beispiel 7.10. `cluster.conf` mit hinzugefügten Diensten: Einer verwendet globale Ressourcen, der andere verwendet dienstspezifische Ressourcen

```
<cluster name="mycluster" config_version="3">
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
       <failoverdomains>
           <failoverdomain name="example_pri" nofailback="0" ordered="1"
restricted="0">
               <failoverdomainnode name="node-01.example.com" priority="1"/>
               <failoverdomainnode name="node-02.example.com" priority="2"/>
               <failoverdomainnode name="node-03.example.com" priority="3"/>
           </failoverdomain>
       </failoverdomains>
       <resources>
           <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3"/>
           <ip address="127.143.131.100" monitor_link="yes" sleeptime="10"/>
           <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
       </resources>
       <service autostart="1" domain="example_pri" exclusive="0"
name="example_apache" recovery="relocate">
           <fs ref="web_fs"/>
           <ip ref="127.143.131.100"/>
           <apache ref="example_server"/>
       </service>
       <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache2" recovery="relocate">
           <fs name="web_fs2" device="/dev/sdd3" mountpoint="/var/www2"
fstype="ext3"/>
           <ip address="127.143.131.101" monitor_link="yes" sleeptime="10"/>
           <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
       </service>
   </rm>
</cluster>
```

7.6. Konfiguration von Redundant Ring Protocol

Ab Red Hat Enterprise Linux 6.4 unterstützt das Red Hat Hochverfügbarkeits-Add-On die Konfiguration des Redundant Ring Protocols.

Bei der Konfiguration eines Systems zur Verwendung des Redundant Ring Protocols müssen Sie die folgenden Faktoren berücksichtigen:

- Legen Sie nicht mehr als zwei Ringe an.
- Jeder Ring muss das gleiche Protokoll verwenden; Sie dürfen nicht IPv4 und IPv6 mischen.
- Wenn nötig, können Sie manuell eine Multicast-Adresse für den zweiten Ring angeben. Wenn Sie eine Multicast-Adresse für den zweiten Ring angeben, muss entweder die alternative Multicast-Adresse oder der alternative Port anders sein als die Multicast-Adresse für den ersten Ring. Wenn Sie keine alternative Multicast-Adresse angeben haben, wird das System automatisch eine andere Multicast-Adresse für den zweiten Ring verwenden.

  Wenn Sie einen alternativen Port angeben, müssen die Port-Nummern des ersten Rings und des zweiten Rings um mindestens zwei unterschiedlich sein, da das System selbst port und port-1 verwendet, um Operationen durchzuführen.
- Verwenden Sie nicht zwei unterschiedliche Schnittstellen auf demselben Subnetz.
- Im Allgemeinen ist es ist ratsam, das Redundant Ring Protocol auf zwei unterschiedlichen Netzwerkkarten und zwei verschiedenen Switches zu konfigurieren, für den Fall, dass eine Netzwerkkarte oder ein Switch ausfällt.
- Verwenden Sie nicht den **ifdown** oder den **service network stop** Befehl, um einen Netzwerkausfall zu simulieren. Dies zerstört den ganzen Cluster und erfordert, dass Sie alle Knoten im Cluster neu starten müssen, um ihn wiederherzustellen.
- Verwenden Sie nicht den **NetworkManager**, da es den **ifdown** Befehl durchführt, wenn das Kabel herausgezogen wird.
- Wenn ein Knoten einer Netzwerkkarte ausfällt, wird der gesamte Ring als ausgefallen markiert.
- Manuelles Eingreifen ist nicht erforderlich, um einen ausgefallenen Ring wiederherzustellen. Zur Wiederherstellung brauchen Sie nur den Grund für den Ausfall, wie z.B. eine ausgefallene Netzwerkkarte oder Switch, zu beheben.

Um eine zweite Netzwerkschnittstelle zur Verwendung des Redundant Ring Protocols festzulegen, fügen Sie eine **altname** Komponente zum **clusternode** Abschnitt der **cluster.conf** Konfigurationsdatei hinzu. Wenn Sie **altname** festlegen, müssen Sie einen **name** Parameter definieren, um einen zweiten Host-Namen oder die IP-Adresse des Knotens anzugeben.

Im folgenden Beispiel wird **clusternet-node1-eth2** als der alternative Name für den Cluster-Knoten **clusternet-node1-eth1** definiert.

```
<cluster name="mycluster" config_version="3" >
  <logging debug="on"/>
  <clusternodes>
    <clusternode name="clusternet-node1-eth1" votes="1" nodeid="1">
      <fence>
        <method name="single">
          <device name="xvm" domain="clusternet-node1"/>
        </method>
      </fence>
      <altname name="clusternet-node1-eth2"/>
    </clusternode>
```

Der **altname** Abschnitt innerhalb des **clusternode** Block ist nicht positionsabhängig. Es kann vor oder nach dem **fence** Abschnitt kommen. Definieren Sie nicht mehr als eine **altname** Komponente für einen Cluster-Knoten, andernfalls kann das System nicht gestartet werden.

Wahlweise können Sie eine Multicast-Adresse, einen Port und eine TTL manuell für den zweiten Ring angeben, indem Sie eine **altmulticast** Komponente im **cman** Abschnitt der **cluster.conf** Konfigurationsdatei definieren. Die **altmulticast** Komponente akzeptiert einen **addr**, einen **port**, und einen **ttl** Parameter.

Das folgende Beispiel zeigt den **cman** Abschnitt einer Cluster-Konfigurationsdatei, die eine Multicast-Adresse, Port und TTL für den zweiten Ring festlegt.

```
<cman>
   <multicast addr="239.192.99.73" port="666" ttl="2"/>
   <altmulticast addr="239.192.99.88" port="888" ttl="3"/>
</cman>
```

7.7. Konfiguration von Debugging-Optionen

Sie können Debugging für alle Daemons in einem Cluster aktivieren, oder Sie können Protokollierung für bestimmte Cluster-Prozesse aktivieren.

Um Debugging für alle Daemons zu aktivieren, fügen Sie Folgendes zur **/etc/cluster/cluster.conf** Datei hinzu. Standardmäßig wird Protokollausgabe in die Datei **/var/log/cluster/*daemon*.log** geschrieben.

```
<cluster config_version="7" name="rh6cluster">
  <logging debug="on"/>
   ...
</cluster>
```

Um Debugging für einzelne Cluster-Prozesse zu aktivieren, fügen Sie die folgenden Zeilen zur **/etc/cluster/cluster.conf** Datei hinzu. Die Konfiguration für einzelne Daemons setzt dabei die globalen Einstellungen außer Kraft.

```
<cluster config_version="7" name="rh6cluster">
   ...
  <logging>
       <!-- turning on per-subsystem debug logging -->
       <logging_daemon name="corosync" debug="on" />
       <logging_daemon name="fenced" debug="on" />
       <logging_daemon name="qdiskd" debug="on" />
       <logging_daemon name="rgmanager" debug="on" />
       <logging_daemon name="dlm_controld" debug="on" />
       <logging_daemon name="gfs_controld" debug="on" />
  </logging>
   ...
</cluster>
```

Eine Liste der Daemons, für die Sie die Protokollierung aktivieren können, sowie die zusätzlichen Protokollierungsoptionen, die Sie sowohl global als auch für einzelne Daemons konfigurieren können, finden Sie auf der **cluster.conf**(5) Handbuchseite.

7.8. Konfiguration von nfsexport- und nfsserver-Ressourcen

Dieser Abschnitt beschreibt Probleme und Überlegungen, die bei der Konfiguration einer **nfsexport**-

oder **nfsserver**-Ressource in Erwägung gezogen werden sollten.

Der **nfsexport**-Ressourcen-Agent funktioniert mit NFSv2- und NFSv3-Clients. Um **nfsexport** zu verwenden, müssen Sie Folgendes tun:

- Vergewissern Sie sich, dass **nfs** und **nfslock** beim Systemstart aktiviert sind.
- Fügen Sie auf allen Cluster-Knoten **RPCNFSDARGS="-N 4"** zur **/etc/sysconfig/nfs** Datei hinzu.
- Fügen Sie **nfslock="1"** zur **service** Komponente in der **cluster.conf** Datei hinzu.
- Strukturieren Sie Ihren Dienst wie folgt:

```
<service nfslock="1" ... >
  <fs name="myfs" ... >
    <nfsexport name="exports">
      <nfsclient ref="client1" />
      <nfsclient ref="client2" />
      ...
    </nfsexport>
  </fs>
  <ip address="10.1.1.2" />
  ...
</service>
```

Der **nfsserver** Ressourcen-Agent funktioniert mit NFSv3- und NFSv4-Clients. Um **nfsserver** zu verwenden, müssen Sie Folgendes tun:

- Vergewissern Sie sich, dass **nfs** und **nfslock** beim Systemstart deaktiviert sind.
- Vergewissern Sie sich, dass **nfslock="1"** nicht für den Dienst eingestellt ist.
- Strukturieren Sie Ihren Dienst wie folgt:

```
<service ... >
  <fs name="myfs" ... >
    <nfsserver name="server">
      <nfsclient ref="client1" />
      <nfsclient ref="client2" />
      ...
    </nfsexport>
  </fs>
  <ip address="10.1.1.2" />
  ...
</service>
```

Wenn Sie ein System zur Verwendung des **nfsserver** Ressourcen-Agents mit NFSv3 und NFSv4 konfigurieren, müssen Sie die folgenden Einschränkungen berücksichtigen:

- Konfigurieren Sie nur eine **nfsserver** Ressource pro Cluster. Falls Sie mehr benötigen, müssen Sie eingeschränkte Ausfallsicherungs-Domains verwenden um sicherzustellen, dass die zwei fraglichen Dienste *nie* auf demselben Rechner starten können.
- Referenzieren Sie eine global konfigurierte **nfsserver** Ressource in maximal einem Dienst.
- Mischen Sie in demselben Cluster keine alten NFS-Dienste mit dem neuen **nfsserver**. Ältere NFS-Dienste erfordern laufende NFS-Daemons, **nfsserver** erfordert dagegen, dass diese Daemons gestoppt sind, wenn der Dienst gestartet wird.
- Wenn Sie mehrere Dateisysteme verwenden, können Sie keine Vererbung für die Exporte nutzen, daher können Sie **nfsclient** Ressourcen in Diensten mit mehreren Dateisystemen nur begrenzt wiederverwenden. Sie können jedoch explizit Ziel- und Pfadparameter für eine beliebige Anzahl von

nfsclients definieren.

7.9. Überprüfen der Konfiguration

Nachdem Sie Ihre Cluster-Konfigurationsdatei erstellt haben, überprüfen Sie, ob diese einwandfrei funktioniert, indem Sie die folgenden Schritte ausführen:

1. Führen Sie auf jedem Knoten einen Neustart der Cluster-Software aus. Dadurch wird sichergestellt, dass auch solche Konfigurationsänderungen, die nur beim Start überprüft werden, für die aktuelle Konfiguration berücksichtigt werden. Sie können die Cluster-Software durch Ausführen von **service cman restart** neu starten. Zum Beispiel:

```
[root@example-01 ~]# service cman restart
Stopping cluster:
   Leaving fence domain...                                 [  OK  ]
   Stopping gfs_controld...                                [  OK  ]
   Stopping dlm_controld...                                [  OK  ]
   Stopping fenced...                                      [  OK  ]
   Stopping cman...                                        [  OK  ]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK  ]
   Unmounting configfs...                                  [  OK  ]
Starting cluster:
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
```

2. Führen Sie **service clvmd start** aus, falls CLVM zum Erstellen geclusterter Datenträger verwendet wird. Zum Beispiel:

```
[root@example-01 ~]# service clvmd start
Activating VGs:                                            [  OK  ]
```

3. Führen Sie **service gfs2 start** aus, falls Sie Red Hat GFS2 verwenden. Zum Beispiel:

```
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK  ]
```

4. Führen Sie **service rgmanager start** aus, falls Sie Hochverfügbarkeitsdienste verwenden. Zum Beispiel:

```
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK  ]
```

5. Führen Sie auf einem beliebigen Cluster-Knoten **cman_tool nodes** aus, um zu überprüfen, dass die Knoten nun als Mitglieder im Cluster fungieren (gekennzeichnet durch ein "M" in der Statusspalte "Sts"). Zum Beispiel:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
   3   M    544   2010-09-28 10:52:21  node-03.example.com
```

6. Überprüfen Sie auf einem beliebigen Knoten mithilfe des **`clustat`** Dienstprogramms, ob die Hochverfügbarkeitsdienste wie erwartet funktionieren. Zusätzlich zeigt **`clustat`** den Status der Cluster-Knoten. Zum Beispiel:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local, rgmanager

 Service Name                   Owner (Last)                   State
 ------- ----                   ----- ------                   -----
 service:example_apache         node-01.example.com            started
 service:example_apache2        (none)                         disabled
```

7. Wenn der Cluster wie erwartet funktioniert, sind Sie mit dem Erstellen der Konfigurationsdatei fertig. Sie können den Cluster mit den in Kapitel 8, *Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools* beschriebenen Befehlszeilen-Tools verwalten.

Kapitel 8. Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools

Dieses Kapitel erläutert die verschiedenen administrativen Aufgaben zur Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons und umfasst die folgenden Abschnitte:

- Abschnitt 8.1, „Starten und Stoppen der Cluster-Software“
- Abschnitt 8.2, „Hinzufügen oder Löschen eines Knotens“
- Abschnitt 8.3, „Verwaltung von Hochverfügbarkeitsdiensten“
- Abschnitt 8.4, „Aktualisieren einer Konfiguration“



Wichtig

Stellen Sie sicher, dass Ihre Bereitstellung des Red Hat Hochverfügbarkeits-Add-Ons Ihren Anforderungen gerecht wird und unterstützt werden kann. Beratschlagen Sie sich dazu ggf. mit einem autorisierten Red Hat Vertreter, um Ihre Konfiguration vor der Bereitstellung zu prüfen. Berücksichtigen Sie zudem eine gewisse Zeit für einen Burn-In-Test, um die Konfiguration auf mögliche Ausfälle zu überprüfen.



Wichtig

Dieses Kapitel verweist auf häufig verwendete **cluster.conf** Elemente und Parameter. Eine vollständige Liste samt Beschreibung aller **cluster.conf** Elemente und Parameter finden Sie im Cluster-Schema unter **/usr/share/cluster/cluster.rng** und das kommentierte Schema unter **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (zum Beispiel **/usr/share/doc/cman-3.0.12/cluster_conf.html**).



Wichtig

Bestimmte Verfahren in diesem Kapitel erfordern, dass der **cman_tool version -r** Befehl zum Verbreiten der Cluster-Konfiguration im gesamten Cluster ausgeführt wird. Für die Verwendung dieses Befehls ist es erforderlich, dass **ricci** läuft.



Anmerkung

Einige Verfahren in diesem Kapitel enthalten bestimmte Befehle für die in Anhang E, *Überblick über Befehlszeilen-Tools* aufgelisteten Befehlszeilen-Tools. Weitere Informationen über alle Befehle und Variablen finden Sie auf der Handbuchseite des jeweiligen Befehlszeilen-Tools.

8.1. Starten und Stoppen der Cluster-Software

Sie können die Cluster-Software auf einem Knoten gemäß Abschnitt 8.1.1, „Starten der Cluster-Software“ und Abschnitt 8.1.2, „Stoppen der Cluster-Software“ starten und stoppen. Das Starten der Cluster-Software auf einem Knoten veranlasst diesen dazu, dem Cluster beizutreten; das Stoppen der Cluster-Software auf einem Knoten veranlasst ihn dazu, den Cluster zu verlassen.

8.1.1. Starten der Cluster-Software

Um die Cluster-Software auf einem Knoten zu starten, führen Sie die folgenden Befehle in der angegebenen Reihenfolge aus:

1. **service cman start**
2. **service clvmd start**, falls CLVM zum Erstellen geclusterter Datenträger verwendet wird
3. **service gfs2 start**, falls Sie Red Hat GFS2 verwenden
4. **service rgmanager start**, falls Sie Hochverfügbarkeitsdienste verwenden (**rgmanager**)

Zum Beispiel:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                            [  OK  ]
Activating VG(s):   2 logical volume(s) in volume group "vg_example" now active
                                                           [  OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK  ]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]#
```

8.1.2. Stoppen der Cluster-Software

Um die Cluster-Software auf einem Knoten zu stoppen, führen Sie die folgenden Befehle in der angegebenen Reihenfolge aus:

1. **service rgmanager stop**, falls Sie Hochverfügbarkeitsdienste verwenden (**rgmanager**)
2. **service gfs2 stop**, falls Sie Red Hat GFS2 verwenden
3. **umount -at gfs2**, falls Sie Red Hat GFS2 in Verbindung mit dem **rgmanager** verwenden, um sicherzustellen, dass jegliche GFS2-Dateien, die während des Starts von **rgmanager** eingehängt wurden (jedoch beim Beenden nicht ausgehängt wurden) ebenfalls ausgehängt werden.
4. **service clvmd stop**, falls CLVM zum Erstellen geclusterter Datenträger verwendet wird
5. **service cman stop**

Zum Beispiel:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK  ]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK  ]
[root@example-01 ~]# umount -at gfs2
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [  OK  ]
clvmd terminated                                           [  OK  ]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [  OK  ]
   Stopping gfs_controld...                                [  OK  ]
   Stopping dlm_controld...                                [  OK  ]
   Stopping fenced...                                      [  OK  ]
   Stopping cman...                                        [  OK  ]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK  ]
   Unmounting configfs...                                  [  OK  ]
[root@example-01 ~]#
```



Anmerkung

Durch das Stoppen der Cluster-Software auf einem Knoten wechseln dessen Hochverfügbarkeitsdienste auf einen anderen Knoten. Alternativ dazu können Sie in Erwägung ziehen, die Hochverfügbarkeitsdienste vor dem Stoppen der Cluster-Software auf einen anderen Knoten zu verlegen oder zu migrieren. Informationen über das Verwalten von Hochverfügbarkeitsdiensten finden Sie in Abschnitt 8.3, „Verwaltung von Hochverfügbarkeitsdiensten“.

8.2. Hinzufügen oder Löschen eines Knotens

Dieser Abschnitt beschreibt, wie ein Knoten von einem Cluster entfernt wird und wie ein Knoten zu einem Cluster hinzugefügt wird. Sie können einen Knoten von einem Cluster löschen gemäß Abschnitt 8.2.1, „Einen Knoten vom Cluster löschen“; und Sie können einen Knoten zu einem Cluster hinzufügen gemäß Abschnitt 8.2.2, „Einen Knoten zum Cluster hinzufügen“.

8.2.1. Einen Knoten vom Cluster löschen

Das Löschen eines Knotens vom Cluster umfasst das Stoppen der Cluster-Software auf dem zu löschenden Knoten und das Aktualisieren der Cluster-Konfiguration, um die Änderung widerzuspiegeln.



Wichtig

Falls der Cluster durch das Löschen eines Knotens nunmehr nur noch zwei Knoten umfasst, müssen Sie die Cluster-Software auf beiden Knoten nach Änderung der Konfigurationsdatei neu starten.

Um einen Knoten von einem Cluster zu löschen, führen Sie die folgenden Schritte aus:

1. Verwenden Sie auf einem beliebigen Knoten das **clusvcadm** Dienstprogramm, um alle Hochverfügbarkeitsdienste, die auf dem zu löschenden Knoten laufen, entweder zu verlegen, zu migrieren oder zu stoppen. Weitere Informationen zur Verwendung von **clusvcadm** finden Sie in Abschnitt 8.3, „Verwaltung von Hochverfügbarkeitsdiensten“.
2. Halten Sie auf dem zu löschenden Knoten die Cluster-Software gemäß Abschnitt 8.1.2, „Stoppen der Cluster-Software“ an. Zum Beispiel:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK  ]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK  ]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [  OK  ]
clvmd terminated                                           [  OK  ]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [  OK  ]
   Stopping gfs_controld...                                [  OK  ]
   Stopping dlm_controld...                                [  OK  ]
   Stopping fenced...                                      [  OK  ]
   Stopping cman...                                        [  OK  ]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK  ]
   Unmounting configfs...                                  [  OK  ]
[root@example-01 ~]#
```

3. Bearbeiten Sie auf einem beliebigen Knoten im Cluster die **/etc/cluster/cluster.conf**, um den **clusternode** Abschnitt des zu löschenden Knotens zu entfernen. Falls z.B. node-03.example.com in Beispiel 8.1, „Drei-Knoten-Cluster-Konfiguration“ entfernt werden soll, löschen Sie den **clusternode** Abschnitt für diesen Knoten. Falls der Cluster durch das Löschen eines Knotens nunmehr nur noch zwei Knoten umfasst, können Sie die folgende Zeile zur Konfigurationsdatei hinzufügen, damit ein einzelner Knoten das Quorum erhalten kann (falls z.B. ein Knoten ausfällt):

   <cman two_node="1" expected_votes="1"/>

   Siehe Abschnitt 8.2.3, „Beispiele für Drei-Knoten- und Zwei-Knoten-Konfigurationen“ für einen Vergleich einer Drei-Knoten- und einer Zwei-Knoten-Konfiguration.

4. Aktualisieren Sie den **config_version** Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von **config_version="2"** auf **config_version="3"**).
5. Speichern Sie die **/etc/cluster/cluster.conf** ab.
6. **(Optional)** Überprüfen Sie die aktualisierte Datei anhand des Cluster-Schemas (**cluster.rng**), indem Sie den **ccs_config_validate** Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

7. Führen Sie den **cman_tool version -r** Befehl durch, um die Konfiguration an die übrigen Cluster-Knoten weiterzugeben.
8. Vergewissern Sie sich, dass die aktualisierte Konfigurationsdatei übertragen wurde.
9. Falls der Cluster durch das Löschen eines Knotens nunmehr nur noch zwei Knoten umfasst, müssen Sie die Cluster-Software wie folgt neu starten:
   a. Halten Sie auf jedem Knoten die Cluster-Software gemäß Abschnitt 8.1.2, „Stoppen der Cluster-Software“ an. Zum Beispiel:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK  ]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK  ]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [  OK  ]
clvmd terminated                                           [  OK  ]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [  OK  ]
   Stopping gfs_controld...                                [  OK  ]
   Stopping dlm_controld...                                [  OK  ]
   Stopping fenced...                                      [  OK  ]
   Stopping cman...                                        [  OK  ]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK  ]
   Unmounting configfs...                                  [  OK  ]
[root@example-01 ~]#
```

b. Starten Sie auf jedem Knoten die Cluster-Software gemäß Abschnitt 8.1.1, „Starten der Cluster-Software“. Zum Beispiel:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                            [  OK  ]
Activating VG(s):   2 logical volume(s) in volume group "vg_example"
now active
                                                           [  OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK  ]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]#
```

c. Führen Sie auf einem beliebigen Cluster-Knoten **`cman_tool nodes`** aus, um zu überprüfen, dass die Knoten nun als Mitglieder im Cluster fungieren (gekennzeichnet durch ein "M" in der Statusspalte "Sts"). Zum Beispiel:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
```

d. Überprüfen Sie auf einem beliebigen Knoten mithilfe des **`clustat`** Dienstprogramms, ob die Hochverfügbarkeitsdienste wie erwartet funktionieren. Zusätzlich zeigt **`clustat`** den Status der Cluster-Knoten. Zum Beispiel:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-02.example.com                        2 Online, rgmanager
 node-01.example.com                        1 Online, Local,
rgmanager

 Service Name                   Owner (Last)                   State
 ------- ----                   ----- ------                   -----
 service:example_apache        node-01.example.com            started
 service:example_apache2       (none)                         disabled
```

8.2.2. Einen Knoten zum Cluster hinzufügen

Das Hinzufügen eines Knotens zum Cluster umfasst das Aktualisieren der Cluster-Konfiguration, das Übertragen der aktualisierten Konfiguration auf den hinzuzufügenden Knoten, und das Starten der Cluster-Software auf diesem Knoten. Um einen Knoten zu einem Cluster hinzuzufügen, führen Sie die folgenden Schritte aus:

1. Bearbeiten Sie auf einem beliebigen Knoten im Cluster die **/etc/cluster/cluster.conf** Datei, um einen **clusternode** Abschnitt für den neuen Knoten hinzuzufügen. Um in Beispiel 8.2, „Zwei-Knoten-Cluster-Konfiguration" beispielsweise node-03.example.com hinzuzufügen, fügen Sie einen **clusternode** Abschnitt für diesen Knoten ein. Falls der Cluster durch das Hinzufügen eines Knotens von vormals zwei Knoten auf nun drei oder mehr Knoten anwächst, entfernen Sie die folgenden **cman** Parameter aus der **/etc/cluster/cluster.conf**:
   - **cman two_node="1"**
   - **expected_votes="1"**

   Siehe Abschnitt 8.2.3, „Beispiele für Drei-Knoten- und Zwei-Knoten-Konfigurationen" für einen Vergleich einer Drei-Knoten- und einer Zwei-Knoten-Konfiguration.
2. Aktualisieren Sie den **config_version** Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von **config_version="2"** auf **config_version="3"**).
3. Speichern Sie die **/etc/cluster/cluster.conf** ab.
4. **(Optional)** Überprüfen Sie die aktualisierte Datei anhand des Cluster-Schemas (**cluster.rng**), indem Sie den **ccs_config_validate** Befehl ausführen. Zum Beispiel:

   ```
   [root@example-01 ~]# ccs_config_validate
   Configuration validates
   ```
5. Führen Sie den **cman_tool version -r** Befehl durch, um die Konfiguration an die übrigen Cluster-Knoten weiterzugeben.
6. Vergewissern Sie sich, dass die aktualisierte Konfigurationsdatei übertragen wurde.
7. Übertragen Sie die aktualisierte Konfigurationsdatei nach **/etc/cluster/** in jedem Knoten, der zum Cluster hinzugefügt werden soll. Verwenden Sie beispielsweise den **scp** Befehl, um die aktualisierte Konfigurationsdatei auf jeden hinzuzufügenden Knoten zu übertragen.
8. Falls die Anzahl der Knoten im Cluster durch das Hinzufügen von Knoten nunmehr mehr als zwei Knoten umfasst, müssen Sie die Cluster-Software in den vorhandenen Cluster-Knoten wie folgt neu starten:
   a. Halten Sie auf jedem Knoten die Cluster-Software gemäß Abschnitt 8.1.2, „Stoppen der Cluster-Software" an. Zum Beispiel:

```
[root@example-01 ~]# service rgmanager stop
Stopping Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]# service gfs2 stop
Unmounting GFS2 filesystem (/mnt/gfsA):                    [  OK  ]
Unmounting GFS2 filesystem (/mnt/gfsB):                    [  OK  ]
[root@example-01 ~]# service clvmd stop
Signaling clvmd to exit                                    [  OK  ]
clvmd terminated                                           [  OK  ]
[root@example-01 ~]# service cman stop
Stopping cluster:
   Leaving fence domain...                                 [  OK  ]
   Stopping gfs_controld...                                [  OK  ]
   Stopping dlm_controld...                                [  OK  ]
   Stopping fenced...                                      [  OK  ]
   Stopping cman...                                        [  OK  ]
   Waiting for corosync to shutdown:                       [  OK  ]
   Unloading kernel modules...                             [  OK  ]
   Unmounting configfs...                                  [  OK  ]
[root@example-01 ~]#
```

b. Starten Sie auf jedem Knoten die Cluster-Software gemäß Abschnitt 8.1.1, „Starten der Cluster-Software“. Zum Beispiel:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                             [  OK  ]
   Global setup...                                         [  OK  ]
   Loading kernel modules...                               [  OK  ]
   Mounting configfs...                                    [  OK  ]
   Starting cman...                                        [  OK  ]
   Waiting for quorum...                                   [  OK  ]
   Starting fenced...                                      [  OK  ]
   Starting dlm_controld...                                [  OK  ]
   Starting gfs_controld...                                [  OK  ]
   Unfencing self...                                       [  OK  ]
   Joining fence domain...                                 [  OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                            [  OK  ]
Activating VG(s):   2 logical volume(s) in volume group "vg_example"
now active
                                                           [  OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                      [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                      [  OK  ]
[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                          [  OK  ]
[root@example-01 ~]#
```

9. Starten Sie auf jedem Knoten, der zum Cluster hinzugefügt werden soll, die Cluster-Software gemäß Abschnitt 8.1.1, „Starten der Cluster-Software“. Zum Beispiel:

```
[root@example-01 ~]# service cman start
Starting cluster:
   Checking Network Manager...                                [  OK  ]
   Global setup...                                            [  OK  ]
   Loading kernel modules...                                  [  OK  ]
   Mounting configfs...                                       [  OK  ]
   Starting cman...                                           [  OK  ]
   Waiting for quorum...                                      [  OK  ]
   Starting fenced...                                         [  OK  ]
   Starting dlm_controld...                                   [  OK  ]
   Starting gfs_controld...                                   [  OK  ]
   Unfencing self...                                          [  OK  ]
   Joining fence domain...                                    [  OK  ]
[root@example-01 ~]# service clvmd start
Starting clvmd:                                               [  OK  ]
Activating VG(s):   2 logical volume(s) in volume group "vg_example" now
active
                                                              [  OK  ]
[root@example-01 ~]# service gfs2 start
Mounting GFS2 filesystem (/mnt/gfsA):                         [  OK  ]
Mounting GFS2 filesystem (/mnt/gfsB):                         [  OK  ]

[root@example-01 ~]# service rgmanager start
Starting Cluster Service Manager:                             [  OK  ]
[root@example-01 ~]#
```

10. Überprüfen Sie auf einem beliebigen Knoten mithilfe des **clustat** Dienstprogramms, dass jeder hinzugefügte Knoten läuft und Teil des Clusters ist. Zum Beispiel:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local, rgmanager

 Service Name                  Owner (Last)                   State
 ------- ----                  ----- ------                   -----
 service:example_apache        node-01.example.com            started
 service:example_apache2       (none)                         disabled
```

Informationen über die Verwendung von **clustat** finden Sie in Abschnitt 8.3, „Verwaltung von Hochverfügbarkeitsdiensten“.

Zusätzlich können Sie **cman_tool status** dazu verwenden, um die Knotenstimmen, Knotenanzahl und Quorum-Zahl zu überprüfen. Zum Beispiel:

```
[root@example-01 ~]#cman_tool status
Version: 6.2.0
Config Version: 19
Cluster Name: mycluster
Cluster Id: 3794
Cluster Member: Yes
Cluster Generation: 548
Membership state: Cluster-Member
Nodes: 3
Expected votes: 3
Total votes: 3
Node votes: 1
Quorum: 2
Active subsystems: 9
Flags:
Ports Bound: 0 11 177
Node name: node-01.example.com
Node ID: 3
Multicast addresses: 239.192.14.224
Node addresses: 10.15.90.58
```

11. Sie können auf einem beliebigen Knoten das **clusvcadm** Dienstprogramm verwenden, um einen laufenden Dienst auf den neu beigetretenen Knoten zu verlegen oder zu migrieren. Sie können auch eventuell deaktivierte Dienste aktivieren. Informationen über die Verwendung von **clusvcadm** finden Sie in Abschnitt 8.3, „Verwaltung von Hochverfügbarkeitsdiensten“

8.2.3. Beispiele für Drei-Knoten- und Zwei-Knoten-Konfigurationen

Für einen Vergleich einer Drei-Knoten- und einer Zwei-Knoten-Konfiguration siehe die nachfolgenden Beispiele.

Beispiel 8.1. Drei-Knoten-Cluster-Konfiguration

```
<cluster name="mycluster" config_version="3">
   <cman/>
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
     </clusternode>
     <clusternode name="node-03.example.com" nodeid="3">
         <fence>
            <method name="APC">
              <device name="apc" port="3"/>
            </method>
         </fence>
     </clusternode>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
       <failoverdomains>
           <failoverdomain name="example_pri" nofailback="0" ordered="1"
restricted="0">
               <failoverdomainnode name="node-01.example.com" priority="1"/>
               <failoverdomainnode name="node-02.example.com" priority="2"/>
               <failoverdomainnode name="node-03.example.com" priority="3"/>
           </failoverdomain>
       </failoverdomains>
       <resources>
           <ip address="127.143.131.100" monitor_link="yes" sleeptime="10">
              <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3">
                 <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
              </fs>
           </ip>
       </resources>
       <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache" recovery="relocate">
           <fs ref="web_fs"/>
           <ip ref="127.143.131.100"/>
           <apache ref="example_server"/>
       </service>
       <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache2" recovery="relocate">
           <fs name="web_fs2" device="/dev/sdd3" mountpoint="/var/www"
fstype="ext3"/>
           <ip address="127.143.131.101" monitor_link="yes" sleeptime="10"/>
           <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
       </service>
   </rm>
</cluster>
```

Beispiel 8.2. Zwei-Knoten-Cluster-Konfiguration

```
<cluster name="mycluster" config_version="3">
   <cman two_node="1" expected_votes="1"/>
   <clusternodes>
     <clusternode name="node-01.example.com" nodeid="1">
         <fence>
            <method name="APC">
              <device name="apc" port="1"/>
             </method>
         </fence>
     </clusternode>
     <clusternode name="node-02.example.com" nodeid="2">
         <fence>
            <method name="APC">
              <device name="apc" port="2"/>
            </method>
         </fence>
   </clusternodes>
   <fencedevices>
         <fencedevice agent="fence_apc" ipaddr="apc_ip_example"
login="login_example" name="apc" passwd="password_example"/>
   </fencedevices>
   <rm>
       <failoverdomains>
           <failoverdomain name="example_pri" nofailback="0" ordered="1"
restricted="0">
               <failoverdomainnode name="node-01.example.com" priority="1"/>
               <failoverdomainnode name="node-02.example.com" priority="2"/>
           </failoverdomain>
       </failoverdomains>
       <resources>
           <ip address="127.143.131.100" monitor_link="yes" sleeptime="10">
              <fs name="web_fs" device="/dev/sdd2" mountpoint="/var/www"
fstype="ext3">
                 <apache config_file="conf/httpd.conf" name="example_server"
server_root="/etc/httpd" shutdown_wait="0"/>
              </fs>
           </ip>
       </resources>
       <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache" recovery="relocate">
           <fs ref="web_fs"/>
           <ip ref="127.143.131.100"/>
           <apache ref="example_server"/>
       </service>
       <service autostart="0" domain="example_pri" exclusive="0"
name="example_apache2" recovery="relocate">
           <fs name="web_fs2" device="/dev/sdd3" mountpoint="/var/www"
fstype="ext3"/>
           <ip address="127.143.131.101" monitor_link="yes" sleeptime="10"/>
           <apache config_file="conf/httpd.conf" name="example_server2"
server_root="/etc/httpd" shutdown_wait="0"/>
       </service>
   </rm>
</cluster>
```

8.3. Verwaltung von Hochverfügbarkeitsdiensten

Sie können Hochverfügbarkeitsdienste mithilfe der **Cluster Status Utility**, **`clustat`**, und der **Cluster User Service Administration Utility**, **`clusvcadm`** verwalten. **`clustat`** zeigt den Status eines Clusters und **`clusvcadm`** ermöglicht die Verwaltung von Hochverfügbarkeitsdiensten.

Dieser Abschnitt liefert grundlegende Informationen über die Verwaltung von Hochverfügbarkeitsdiensten mithilfe der **`clustat`** und **`clusvcadm`** Befehle. Er besteht aus den folgenden Unterabschnitten:

- Abschnitt 8.3.1, „Anzeige des Hochverfügbarkeitsdienst-Status mit **`clustat`**“
- Abschnitt 8.3.2, „Verwaltung von Hochverfügbarkeitsdiensten mit **`clusvcadm`**“

8.3.1. Anzeige des Hochverfügbarkeitsdienst-Status mit `clustat`

`clustat` zeigt den clusterweiten Status an. Es zeigt Informationen über Mitgliedschaften, die Quorum-Ansicht, den Status aller Hochverfügbarkeitsdienste, und es gibt außerdem an, auf welchem Knoten der **`clustat`** Befehl ausgeführt wird (lokal). Tabelle 8.1, „Dienst-Status“ beschreibt die Status, in denen sich die Dienste befinden können und die durch Ausführen von **`clustat`** angezeigt werden. Beispiel 8.3, „**`clustat`** Anzeige“ zeigt ein Beispiel einer **`clustat`** Anzeige. Detailliertere Informationen zum Ausführen des **`clustat`** Befehls finden Sie auf der **`clustat`** Handbuchseite.

Tabelle 8.1. Dienst-Status

Dienst-Status	Beschreibung
Started	Die Dienstressourcen sind konfiguriert und stehen dem Cluster-System, das diesen Dienst besitzt, zur Verfügung.
Recovering	Der Dienst wartet darauf, auf einem anderen Knoten zu starten.
Disabled	Der Dienst wurde deaktiviert und ist keinem Besitzer zugewiesen. Ein deaktivierter Dienst wird niemals automatisch vom Cluster neu gestartet.
Stopped	In gestopptem Zustand wird der Dienst für einen Start nach der nächsten Dienst- oder Knotenänderung evaluiert. Es handelt sich um einen vorübergehenden Status. Sie können den Dienst von diesem Status aus deaktivieren oder aktivieren.
Failed	Der Dienst ist vermutlich tot. Ein Dienst wird in diesen Status versetzt, wenn die *stop* Operation einer Ressource fehlschlägt. Nachdem ein Dienst in diesen Status versetzt wurde, müssen Sie sicherstellen, dass keine Ressourcen (z.B. ein eingehängtes Dateisystem) zugewiesen sind, bevor Sie eine **`disable`** Anfrage senden. Die einzige Operation, die auf einem Dienst mit diesem Status ausgeführt werden kann, ist **`disable`**.
Uninitialized	Dieser Status kann in bestimmten Fällen während des Starts und des Ausführens von **`clustat -f`** auftreten.

Beispiel 8.3. `clustat` Anzeige

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:15 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local, rgmanager

 Service Name                  Owner (Last)                  State
 ------- ----                  ----- ------                  -----
 service:example_apache        node-01.example.com           started
 service:example_apache2       (none)                        disabled
```

8.3.2. Verwaltung von Hochverfügbarkeitsdiensten mit `clusvcadm`

Sie können Hochverfügbarkeitsdienste mithilfe des **`clusvcadm`** Befehls verwalten. Damit können Sie die folgenden Operationen ausführen:

- Aktivieren und Starten eines Dienstes
- Deaktivieren eines Dienstes
- Stoppen eines Dienstes
- Einfrieren eines Dienstes
- Einfrieren eines Dienstes aufheben
- Migrieren eines Dienstes (nur für Dienste auf virtuellen Maschinen)
- Verlegen eines Dienstes
- Neustarten eines Dienstes

Tabelle 8.2, „Dienstoperationen“ beschreibt die Operationen im Detail. Eine vollständige Beschreibung dessen, wie diese Operationen ausgeführt werden, finden Sie auf der Handbuchseite des **`clusvcadm`** Dienstprogramms.

Tabelle 8.2. Dienstoperationen

Dienst-Operation	Beschreibung	Befehlssyntax
Enable	Startet den Dienst, optional auf einem bevorzugten Ziel und optional gemäß der Regeln zur Ausfallsicherungs-Domain. Werden weder ein bevorzugtes Ziel noch Regeln zur Ausfallsicherungs-Domain angegeben, so wird der Dienst auf dem lokalen Host gestartet, auf dem **clusvcadm** ausgeführt wird. Falls der ursprüngliche *start* fehlschlägt, verhält sich der Dienst, als ob eine *relocate* Operation angefragt wurde (siehe **Relocate** in dieser Tabelle). Falls die Operation erfolgreich ist, wird der Dienst in den "Started"-Status versetzt.	**clusvcadm -e <service_name>** oder **clusvcadm -e <service_name> -m <member>** (Die -m Option gibt das bevorzugte Zielmitglied an, auf dem der Dienst gestartet werden soll.)
Disable	Stoppt den Dienst und versetzt ihn in den "Disabled"-Zustand. Dies ist die einzig zulässige Operation, wenn sich ein Dienst im *failed* Status befindet.	**clusvcadm -d <service_name>**
Relocate	Verlegt den Dienst auf einen anderen Knoten. Optional können Sie einen bevorzugten Knoten angeben, auf den der Dienst verlegt werden soll. Kann der Dienst nicht auf diesem bevorzugten Knoten ausgeführt werden (z.B. weil der Start des Dienstes fehlschlägt oder der Host offline ist), so verhindert dies jedoch nicht die Verlegung, sondern es wird stattdessen ein anderer Knoten ausgewählt. **rgmanager** versucht, den Dienst auf jedem zulässigen Knoten im Cluster zu starten. Falls keiner der zulässigen Zielknoten im Cluster den Dienst erfolgreich starten kann, schlägt die Verlegung fehl und es wird versucht, den Dienst auf dem ursprünglichen Besitzer neu zu starten. Falls der ursprüngliche Besitzer den Dienst nicht neu starten kann, wird der Dienst in den *stopped* Status versetzt.	**clusvcadm -r <service_name>** oder **clusvcadm -r <service_name> -m <member>** (Die -m Option gibt das bevorzugte Zielmitglied an, auf dem der Dienst gestartet werden soll.)
Stop	Stoppt den Dienst und versetzt ihn in den *stopped* Status.	**clusvcadm -s <service_name>**
Freeze	Friert einen Dienst auf dem Knoten ein, auf dem er derzeit ausgeführt wird. Dies verhindert sowohl Überprüfungen des Dienststatus als auch die Ausfallsicherung, falls der Knoten ausfällt oder rgmanager gestoppt wird. Dies kann verwendet werden, um einen Dienst auszusetzen, wenn Wartungsarbeiten an den zu Grunde liegenden Ressourcen nötig sind. Siehe „Überlegungen zur Verwendung der Freeze- und Unfreeze-	**clusvcadm -Z <service_name>**

	Operationen“ für wichtige Informationen über die Verwendung der *freeze* und *unfreeze* Operationen.	
Unfreeze	Hebt den *freeze* Status eines Dienstes wieder auf. Dadurch werden Überprüfungen des Status wieder ermöglicht. Siehe „Überlegungen zur Verwendung der Freeze- und Unfreeze-Operationen“ für wichtige Informationen über die Verwendung der *freeze* und *unfreeze* Operationen.	`clusvcadm -U <service_name>`
Migrate	Migriert eine virtuelle Maschine auf einen anderen Knoten. Sie müssen dabei einen Zielknoten angeben. Ein Scheitern dieser Migration kann abhängig vom Fehler dazu führen, dass die virtuelle Maschine in den *failed* Zustand oder den "started" Zustand auf dem ursprünglichen Besitzer versetzt wird.	`clusvcadm -M <service_name> -m <member>` **Wichtig** Für die *migrate* Operation *müssen* Sie mithilfe der **`-m <member>`** Option einen Zielknoten spezifizieren.
Restart	Startet einen Dienst auf dem Knoten, auf dem er derzeit ausgeführt wird, neu.	`clusvcadm -R <service_name>`

Überlegungen zur Verwendung der Freeze- und Unfreeze-Operationen

Die Verwendung der *freeze* Operation erlaubt die Wartung von Teilen des **`rgmanager`** Dienstes. Falls Sie beispielsweise eine Datenbank und einen Webserver in einem **`rgmanager`** Dienst haben, können Sie den **`rgmanager`** Dienst einfrieren, die Datenbank stoppen, die Wartungsarbeiten durchführen, die Datenbank neu starten, und das Einfrieren des Dienstes anschließend wieder aufheben.

Wenn ein Dienst eingefroren ist, verhält er sich folgendermaßen:

- *Status*-Überprüfungen sind deaktiviert.
- *Start*-Operationen sind deaktiviert.
- *Stopp*-Operationen sind deaktiviert.
- Es erfolgt keine Ausfallsicherung (selbst wenn Sie den Besitzer des Dienstes ausschalten).



Wichtig

Werden die folgenden Richtlinien nicht befolgt, kann das ggf. dazu führen, dass Ressourcen mehreren Hosts zugewiesen werden:

- Sie *dürfen nicht* alle Instanzen des rgmanager stoppen, wenn ein Dienst eingefroren ist, es sei denn, Sie planen vor dem Neustart von rgmanager einen Neustart der Hosts.
- Sie *dürfen nicht* das Einfrieren eines Dienstes aufheben, bevor der Besitzer des Dienstes wieder dem Cluster beitritt und rgmanager neu startet.

8.4. Aktualisieren einer Konfiguration

Das Aktualisieren der Cluster-Konfiguration umfasst das Bearbeiten der Cluster-Konfigurationsdatei (**`/etc/cluster/cluster.conf`**) und deren Übertragung an alle Knoten im Cluster. Sie können die

Konfiguration unter Verwendung einer der folgenden Verfahren aktualisieren:

- Abschnitt 8.4.1, „Aktualisieren der Konfiguration mittels **cman_tool version -r**“
- Abschnitt 8.4.2, „Aktualisieren der Konfiguration mittels **scp**“

8.4.1. Aktualisieren der Konfiguration mittels cman_tool version -r

Um die Konfiguration mithilfe des Befehls **cman_tool version -r** zu aktualisieren, führen Sie die folgenden Schritte aus:

1. Bearbeiten Sie auf einem beliebigen Knoten im Cluster die **/etc/cluster/cluster.conf** Datei.
2. Aktualisieren Sie den **config_version** Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von **config_version="2"** auf **config_version="3"**).
3. Speichern Sie die **/etc/cluster/cluster.conf** ab.
4. Führen Sie den **cman_tool version -r** Befehl durch, um die Konfiguration an die übrigen Cluster-Knoten zu verbreiten. Es ist notwendig, dass **ricci** auf jedem Cluster-Knoten ausgeführt wird, um die aktualisierten Cluster-Konfigurationsinformationen verbreiten zu können.
5. Vergewissern Sie sich, dass die aktualisierte **cluster.conf** Konfigurationsdatei auf die anderen Knoten im Cluster übertragen wurde. Falls nicht, verwenden Sie den **scp** Befehl, um **/etc/cluster/** auf alle Cluster-Knoten zu verbreiten.
6. Sie können diesen Schritt (Neustart der Cluster-Software) überspringen, falls Sie nur die folgenden Konfigurationsänderungen vorgenommen haben:
   - Löschen eines Knotens aus der Cluster-Konfiguration — *es sei denn*, die Knotenanzahl verringert sich dadurch auf zwei Knoten. Informationen über das Löschen eines Knotens und die Verringerung der Knotenanzahl auf zwei Knoten finden Sie in Abschnitt 8.2, „Hinzufügen oder Löschen eines Knotens“.
   - Hinzufügen eines Knotens zur Cluster-Konfiguration — *es sei denn*, die Knotenanzahl erhöht sich dadurch auf mehr als zwei Knoten. Informationen über das Hinzufügen eines Knotens und die Erhöhung der Knotenanzahl auf mehr als zwei Knoten finden Sie in Abschnitt 8.2.2, „Einen Knoten zum Cluster hinzufügen“.
   - Änderungen an der Protokollierung durch Daemons.
   - Wartung von Hochverfügbarkeitsdiensten/virtuellen Maschinen (hinzufügen, bearbeiten oder löschen).
   - Wartung von Ressourcen (hinzufügen, bearbeiten oder löschen).
   - Wartung von Ausfallsicherungs-Domains (hinzufügen, bearbeiten oder löschen).

   Andernfalls müssen Sie die Cluster-Software wie folgt neu starten:

   a. Halten Sie auf jedem Knoten die Cluster-Software gemäß Abschnitt 8.1.2, „Stoppen der Cluster-Software“ an.
   b. Starten Sie auf jedem Knoten die Cluster-Software gemäß Abschnitt 8.1.1, „Starten der Cluster-Software“.

   Das Stoppen und Starten der Cluster-Software gewährleistet, dass auch solche Konfigurationsänderungen, die nur beim Start überprüft werden, in die laufende Konfiguration miteinbezogen werden.
7. Führen Sie auf einem beliebigen Cluster-Knoten **cman_tool nodes** aus, um zu überprüfen, dass die Knoten nun als Mitglieder im Cluster fungieren (gekennzeichnet durch ein "M" in der Statusspalte "Sts"). Zum Beispiel:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
   3   M    544   2010-09-28 10:52:21  node-03.example.com
```

8. Überprüfen Sie auf einem beliebigen Knoten mithilfe des **clustat** Dienstprogramms, ob die

Hochverfügbarkeitsdienste wie erwartet funktionieren. Zusätzlich zeigt **clustat** den Status der Cluster-Knoten. Zum Beispiel:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local, rgmanager

 Service Name                  Owner (Last)                  State
 ------- ----                  ----- ------                  -----
 service:example_apache        node-01.example.com           started
 service:example_apache2       (none)                        disabled
```

9. Wenn der Cluster wie erwartet funktioniert, sind Sie mit dem Aktualisieren der Konfiguration fertig.

8.4.2. Aktualisieren der Konfiguration mittels scp

Um die Konfiguration mithilfe des **scp** Befehls zu aktualisieren, führen Sie die folgenden Schritte aus:

1. Bearbeiten Sie auf einem beliebigen Knoten im Cluster die **/etc/cluster/cluster.conf** Datei.
2. Aktualisieren Sie den **config_version** Parameter, indem Sie dessen Wert erhöhen (ändern Sie ihn z.B. von **config_version="2"** auf **config_version="3"**).
3. Speichern Sie die **/etc/cluster/cluster.conf** ab.
4. Überprüfen Sie die aktualisierte Datei anhand des Cluster-Schemas (**cluster.rng**), indem Sie den **ccs_config_validate** Befehl ausführen. Zum Beispiel:

```
[root@example-01 ~]# ccs_config_validate
Configuration validates
```

5. Ist die aktualisierte Datei gültig, verwenden Sie den **scp** Befehl, um sie auf **/etc/cluster/** in jedem Cluster-Knoten zu übertragen.
6. Vergewissern Sie sich, dass die aktualisierte Konfigurationsdatei übertragen wurde.
7. Führen Sie den folgenden Befehl auf einem der Cluster-Knoten aus, um die neue Konfiguration zu laden:

```
cman_tool version -r
```

Falls Sie **ricci** nicht installiert haben, können Sie den folgenden Befehl verwenden:

```
cman_tool version -s
```

8. Sie können diesen Schritt (Neustart der Cluster-Software) überspringen, falls Sie nur die folgenden Konfigurationsänderungen vorgenommen haben:
   - Löschen eines Knotens aus der Cluster-Konfiguration — *es sei denn*, die Knotenanzahl verringert sich dadurch auf zwei Knoten. Informationen über das Löschen eines Knotens und die Verringerung der Knotenanzahl auf zwei Knoten finden Sie in Abschnitt 8.2, „Hinzufügen oder Löschen eines Knotens“.
   - Hinzufügen eines Knotens zur Cluster-Konfiguration — *es sei denn*, die Knotenanzahl erhöht sich dadurch auf mehr als zwei Knoten. Informationen über das Hinzufügen eines Knotens und die Erhöhung der Knotenanzahl auf mehr als zwei Knoten finden Sie in Abschnitt 8.2.2, „Einen Knoten zum Cluster hinzufügen“.
   - Änderungen an der Protokollierung durch Daemons.

- Wartung von Hochverfügbarkeitsdiensten/virtuellen Maschinen (hinzufügen, bearbeiten oder löschen).
- Wartung von Ressourcen (hinzufügen, bearbeiten oder löschen).
- Wartung von Ausfallsicherungs-Domains (hinzufügen, bearbeiten oder löschen).

Andernfalls müssen Sie die Cluster-Software wie folgt neu starten:

a. Halten Sie auf jedem Knoten die Cluster-Software gemäß Abschnitt 8.1.2, „Stoppen der Cluster-Software“ an.

b. Starten Sie auf jedem Knoten die Cluster-Software gemäß Abschnitt 8.1.1, „Starten der Cluster-Software“.

Das Stoppen und Starten der Cluster-Software gewährleistet, dass auch solche Konfigurationsänderungen, die nur beim Start überprüft werden, in die laufende Konfiguration miteinbezogen werden.

9. Vergewissern Sie sich, dass die Knoten als Mitglieder im Cluster funktionieren und dass die Hochverfügbarkeitsdienste wie erwartet ausgeführt werden.

a. Führen Sie auf einem beliebigen Cluster-Knoten **cman_tool nodes** aus, um zu überprüfen, dass die Knoten nun als Mitglieder im Cluster fungieren (gekennzeichnet durch ein "M" in der Statusspalte "Sts"). Zum Beispiel:

```
[root@example-01 ~]# cman_tool nodes
Node  Sts   Inc   Joined               Name
   1   M    548   2010-09-28 10:52:21  node-01.example.com
   2   M    548   2010-09-28 10:52:21  node-02.example.com
   3   M    544   2010-09-28 10:52:21  node-03.example.com
```

b. Überprüfen Sie auf einem beliebigen Knoten mithilfe des **clustat** Dienstprogramms, ob die Hochverfügbarkeitsdienste wie erwartet funktionieren. Zusätzlich zeigt **clustat** den Status der Cluster-Knoten. Zum Beispiel:

```
[root@example-01 ~]#clustat
Cluster Status for mycluster @ Wed Nov 17 05:40:00 2010
Member Status: Quorate

 Member Name                             ID   Status
 ------ ----                             ---- ------
 node-03.example.com                         3 Online, rgmanager
 node-02.example.com                         2 Online, rgmanager
 node-01.example.com                         1 Online, Local,
rgmanager

 Service Name                  Owner (Last)                  State
 ------- ----                  ----- ------                  -----
 service:example_apache        node-01.example.com           started
 service:example_apache2       (none)                        disabled
```

Wenn der Cluster wie erwartet funktioniert, sind Sie mit dem Aktualisieren der Konfiguration fertig.

Kapitel 9. Fehlerdiagnose und -behebung in einem Cluster

Cluster-Probleme können schwer zu finden und zu beheben sein, denn ein Cluster mit mehreren Systemen bringt naturgemäß ein höheres Maß an Komplexität mit sich, als dies bei der Problembehebung in einem einzelnen System der Fall ist. Allerdings gibt es bestimmte Probleme, auf die Systemadministratoren bei der Implementierung oder Verwaltung eines Clusters häufig stoßen. Wenn Sie diese häufig auftretenden Probleme und Ihre Lösungen verstehen, kann dies die Implementierung und Verwaltung Ihres Clusters deutlich vereinfachen.

Dieses Kapitel liefert Informationen über einige häufig auftretende Cluster-Probleme sowie deren Lösungen. Weiterführende Hilfe erhalten Sie entweder in unserer Wissensdatenbank oder von einem autorisierten Red Hat Support-Vertreter. Falls Ihr Problem speziell mit dem GFS2-Dateisystem zusammenhängt, können Sie dem Dokument *Global File System 2* weitere Informationen über die Suche und Bereinigung von GFS2-Fehlern entnehmen.

9.1. Konfigurationsänderungen werden nicht wirksam

Wenn Sie Änderungen an einer Cluster-Konfiguration vornehmen, müssen Sie diese Änderungen auf jeden Knoten im Cluster übertragen.

- Wenn Sie einen Cluster mithilfe von **Conga** konfigurieren, überträgt **Conga** die Änderungen automatisch, sobald Sie die Änderungen übernehmen.
- Informationen über das Übertragen der Änderungen an der Cluster-Konfiguration mit dem **ccs** Befehl finden Sie in Abschnitt 5.15, „Verbreiten der Konfigurationsdatei auf den Cluster-Knoten“.
- Informationen über das Übertragen der Änderungen an der Cluster-Konfiguration mit Befehlszeilentools finden Sie in Abschnitt 8.4, „Aktualisieren einer Konfiguration“.

Die folgenden Änderungen an der Konfiguration Ihres Clusters erfordern nach Übertragung der Änderungen keinen Cluster-Neustart, damit die Änderungen wirksam werden.

- Löschen eines Knotens aus der Cluster-Konfiguration — *es sei denn*, die Knotenanzahl verringert sich dadurch von über zwei Knoten auf dann nur noch zwei Knoten.
- Hinzufügen eines Knotens zur Cluster-Konfiguration — *es sei denn*, die Knotenanzahl erhöht sich dadurch von weniger als zwei Knoten auf dann mehr als zwei Knoten.
- Ändern der Protokollierungseinstellungen.
- Hinzufügen, Bearbeiten oder Löschen von HA-Diensten oder VM-Komponenten.
- Hinzufügen, Bearbeiten oder Löschen von Cluster-Ressourcen.
- Hinzufügen, Bearbeiten oder Löschen von Ausfallsicherungs-Domains.

Alle anderen Änderungen an der Konfiguration Ihres Clusters erfordern dagegen nach Übertragung der Änderungen einen Cluster-Neustart, damit die Änderungen wirksam werden. Die folgenden Cluster-Konfiguationsänderungen erfordern einen Cluster-Neustart:

- Hinzufügen oder Entfernen der **two_node** Option aus der Cluster-Konfigurationsdatei.
- Umbenennen des Clusters.
- Ändern von **corosync** oder **openais** Timern.
- Hinzufügen, Ändern oder Löschen von Heuristiken für Quorumdatenträger, Ändern von Quorumdatenträger-Timern oder Ändern des Quorumdatenträgergeräts. Damit diese Änderungen wirksam werden, ist ein globaler Neustart des **qdiskd** Daemons erforderlich.
- Ändern des **central_processing** Modus für **rgmanager**. Damit diese Änderungen wirksam werden, ist ein globaler Neustart von **rgmanager** erforderlich.
- Ändern der Multicast-Adresse.
- Ändern des Transportmodus von UDP-Multicast auf UDP-Unicast oder Ändern des Modus von UDP-Unicast auf UDP-Multicast.

Sie können den Cluster mithilfe von **Conga**, dem **ccs** Befehl oder den Befehlszeilentools neu starten.

- Informationen über das Neustarten eines Clusters mit **Conga** finden Sie in Abschnitt 4.4, „Starten, Stoppen, Neustarten und Löschen von Clustern“.
- Informationen über das Neustarten eines Clusters mit dem **ccs** Befehl finden Sie in Abschnitt 6.2, „Starten und Stoppen eines Clusters“.
- Informationen über das Neustarten eines Clusters mit Befehlszeilentools finden Sie in Abschnitt 8.1, „Starten und Stoppen der Cluster-Software“.

9.2. Cluster wird nicht gebildet

Falls Sie Probleme haben, einen neuen Cluster zu bilden, überprüfen Sie Folgendes:

- Vergewissern Sie sich, dass die Namensauflösung korrekt konfiguriert ist. Der Cluster-Knotenname in der **cluster.conf** Datei sollte mit dem Namen übereinstimmen, der zur Auflösung der Cluster-Netzwerkadresse zur Kommunikation über den Cluster verwendet wird. Falls Ihre Cluster-Knotennamen beispielsweise **nodea** und **nodeb** lauten, dann vergewissern Sie sich, dass für beide Knoten Einträge in der **/etc/cluster/cluster.conf** Datei vorhanden sind und die **/etc/hosts** Datei mit diesen Namen übereinstimmt.
- Falls der Cluster Multicast zur Kommunikation der Knoten untereinander verwendet, stellen Sie sicher, dass auf dem Netzwerk, das der Cluster zur Kommunikation benutzt, Multicast-Datenverkehr nicht blockiert, verzögert oder anderweitig behindert wird. Beachten Sie, dass einige Cisco-Switches über Features verfügen, die ggf. Verzögerungen des Multicast-Datenverkehrs verursachen.
- Verwenden Sie **telnet** oder **SSH**, um zu überprüfen, ob die entfernten Knoten erreichbar sind.
- Führen Sie den **ethtool eth1 | grep link** Befehl durch, um zu überprüfen, ob die Ethernet-Verbindung aktiv ist.
- Verwenden Sie den **tcpdump** Befehl auf jedem Knoten, um den Netzwerkverkehr zu überprüfen.
- Vergewissern Sie sich, dass keine Firewall-Regeln die Kommunikation zwischen Ihren Knoten unterbinden.
- Stellen Sie sicher, dass die Schnittstellen, die der Cluster für die Kommunikation zwischen Knoten benutzt, nur Bindungs-Modus 0, 1 oder 2 verwenden. (Bindungs-Modus 0 und 2 werden ab Red Hat Enterprise Linux 6.4 unterstützt.)

9.3. Knoten können nach Fencing oder Neustart dem Cluster nicht wieder beitreten

Falls Ihre Knoten nach dem Fencing oder einem Neustart dem Cluster nicht wieder beitreten, überprüfen Sie Folgendes:

- Cluster, die Ihre Daten über einen Cisco Catalyst Switch leiten, können ggf. von diesem Problem betroffen sein.
- Vergewissern Sie sich, dass alle Cluster-Knoten dieselbe Version der **cluster.conf** Datei verwenden. Falls die **cluster.conf** Datei auf einem der Knoten abweicht, kann dieser Knoten dem Cluster unter Umständen nicht mehr beitreten.

  Ab Red Hat Enterprise Linux 6.1 können Sie den folgenden Befehl verwenden, um zu überprüfen, ob alle in der Cluster-Konfigurationsdatei des Hosts spezifizierten Knoten über identische Cluster-Konfigurationsdateien verfügen:

  ```
  ccs -h host --checkconf
  ```

  Für Informationen über den **ccs** Befehl, siehe Kapitel 5, *Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit dem **ccs** Befehl* und Kapitel 6, *Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit **ccs***.
- Stellen Sie sicher, dass Sie **chkconfig on** für die Cluster-Dienste in dem Knoten konfiguriert haben, der dem Cluster beizutreten versucht.

- Vergewissern Sie sich, dass keine Firewall-Regeln die Kommunikation zwischen den Knoten im Cluster unterbinden.

9.4. Cluster-Daemon stürzt ab

RGManager verfügt über einen Überwachungsprozess (auch "Watchdog" genannt), der den Host neu startet, falls der **rgmanager** Hauptprozess unerwartet abstürzt. Dies führt dazu, dass der Cluster-Knoten abgegrenzt wird und **rgmanager** den Dienst auf einem anderen Host wiederherstellt. Wenn der Überwachungsdaemon feststellt, dass der **rgmanager** Hauptprozess abgestürzt ist, wird er den Cluster-Knoten neu starten. Die aktiven Cluster-Knoten werden daraufhin bemerken, dass der Cluster-Knoten ausgefallen ist, und ihn aus dem Cluster ausschließen.

Die niedrigere *Prozess-ID* (PID) ist der Überwachungsprozess, der Maßnahmen ergreift, wenn sein Kind (der Prozess mit der höheren PID) abstürzt. Die Erstellung eines Speicherauszugs des Prozesses mit der höheren PID-Nummer mithilfe von **gcore** kann bei der Fehlerbehebung eines abgestürzten Daemons helfen.

Installieren Sie die Pakete, die zum Erstellen und Anzeigen des Speicherauszugs erforderlich sind und vergewissern Sie sich, dass **rgmanager** und **rgmanager-debuginfo** von derselben Version sind, da der Speicherauszug andernfalls möglicherweise unbrauchbar ist.

```
$ yum -y --enablerepo=rhel-debuginfo install gdb rgmanager-debuginfo
```

9.4.1. Erstellen eines rgmanager Speicherauszugs zur Laufzeit

Es gibt zwei **rgmanager** Prozesse, die gestartet werden. Sie müssen den Speicherauszug für den **rgmanager** Prozess mit der höheren PID erstellen.

Sehen Sie nachfolgend eine Beispielausgabe für den **ps** Befehl, die zwei **rgmanager** Prozesse zeigt.

```
$ ps aux | grep rgmanager | grep -v grep

root    22482  0.0  0.5  23544  5136 ?        S<Ls Dec01   0:00 rgmanager
root    22483  0.0  0.2  78372  2060 ?        S<l  Dec01   0:47 rgmanager
```

In dem folgenden Beispiel wird das **pidof** Programm dazu verwendet, um automatisch die höhere PID zu bestimmen, also die, von der der Speicherauszug erstellt werden muss. Der vollständige Befehl erstellt einen Speicherauszug für den Prozess 22483, der die höhere PID-Nummer aufweist.

```
$ gcore -o /tmp/rgmanager-$(date '+%F_%s').core $(pidof -s rgmanager)
```

9.4.2. Erstellen eines Speicherauszugs beim Absturz des Daemons

Standardmäßig blockiert das **/etc/init.d/functions** Skript Speicherauszugsdateien von Daemons, die durch **/etc/init.d/rgmanager** aufgerufen wurden. Damit der Daemon Speicherauszugsdateien erstellen kann, müssen Sie diese Option aktivieren. Diese Prozedur muss auf allen Cluster-Knoten ausgeführt werden, auf denen ein Speicherauszug erstellt werden soll.

Für die Erstellung eines Speicherauszuges, wenn der rgmanager-Daemon abstürzt, bearbeiten Sie die **/etc/sysconfig/cluster** Datei. Der ***DAEMONCOREFILELIMIT*** Parameter erlaubt es dem Daemon, einen Speicherauszug zu erstellen, wenn der Prozess abstürzt. Es gibt eine **-w** Option, die verhindert, dass der Überwachungsprozess läuft. Der Überwachungs-Daemon ist verantwortlich für einen Neustart des Cluster-Knotens, wenn **rgmanager** abstürzt und in einigen Fällen wird der Speicherauszug nicht erzeugt werden, wenn der Überwachungs-Daemon läuft. Aus diesem Grund muss er deaktiviert werden, um Speicherauszüge zu erstellen.

```
DAEMONCOREFILELIMIT="unlimited"
RGMGR_OPTS="-w"
```

Starten Sie rgmanager neu, um die neuen Konfigurationsoptionen zu aktivieren:

```
service rgmanager restart
```



Anmerkung

Falls Cluster-Dienste auf diesem Cluster-Knoten laufen, könnte dies ein Fehlschlagen der laufenden Dienste verursachen.

Die Auszugsdatei wird geschrieben, wenn sie vom Absturz des **rgmanager** Prozesses generiert wird.

```
ls /core*
```

Die Ausgabe sollte etwa wie folgt aussehen:

```
/core.11926
```

Verlegen oder Löschen Sie alte Speicherauszugsdateien im /-Verzeichnis, bevor Sie **rgmanager** neu starten, um einen Speicherauszug der Applikation zu erstellen. Der Cluster-Knoten, auf dem der **rgmanager** Absturz stattfand, sollte neu gestartet oder abgegrenzt werden, nachdem der Speicherauszug erstellt wurde, um sicherzustellen, dass der Überwachungsprozess nicht ausgeführt wurde.

9.4.3. Aufzeichnen einer gdb Backtrace-Sitzung

Nachdem Sie die Speicherauszugsdatei aufgezeichnet haben, können Sie deren Inhalt mithilfe des GNU-Debuggers **gdb** einsehen. Um eine Skriptsitzung von **gdb** auf der Auszugsdatei des betroffenen Systems aufzuzeichnen, führen Sie Folgendes aus:

```
$ script /tmp/gdb-rgmanager.txt
$ gdb /usr/sbin/rgmanager /tmp/rgmanager-.core.
```

Dadurch wird eine **gdb** Sitzung gestartet, die von **script** in der entsprechenden Textdatei aufgezeichnet wird. Führen Sie innerhalb von **gdb** die folgenden Befehle aus:

```
(gdb) thread apply all bt full
(gdb) quit
```

Drücken Sie **Strg-D**, um die Skriptsitzung zu stoppen und sie in der Textdatei zu speichern.

9.5. Cluster-Dienste hängen sich auf

Wenn die Cluster-Dienste einen Knoten abzugrenzen versuchen, werden die Cluster-Dienste gestoppt, bis die Fencing-Operation erfolgreich abgeschlossen wurde. Falls sich also Ihr vom Cluster verwalteter Speicher oder Dienst aufhängt und die Cluster-Knoten unterschiedliche Ansichten der Cluster-Mitgliedschaft zeigen, oder falls Sie einen Knoten abzugrenzen versuchen und Sie zur Wiederherstellung Knoten neu starten müssen, überprüfen Sie, ob die folgenden Gegebenheiten vorliegen:

- Der Cluster hat ggf. versucht, einen Knoten abzugrenzen, und diese Fencing-Operation kann unter Umständen fehlgeschlagen sein.
- Sehen Sie sich die **/var/log/messages** Datei auf allen Knoten an und suchen Sie nach

Nachrichten bezüglich einer fehlgeschlagenen Abgrenzung. Sollten Sie welche finden, starten Sie die Knoten im Cluster neu und konfigurieren Sie das Fencing korrekt.

- Vergewissern Sie sich, dass keine Aufspaltung des Netzwerks auftrat, wie in Abschnitt 9.8, „Jeder Knoten in einem Zwei-Knoten-Cluster meldet den jeweils anderen Knoten als ausgefallen“ beschrieben, und stellen Sie sicher, dass die Kommunikation zwischen den Knoten nach wie vor möglich ist und das Netzwerk aktiv ist.
- Falls Knoten den Cluster verlassen, verfügen die verbleibenden Knoten ggf. über kein Quorum mehr. Der Cluster braucht jedoch ein Quorum, um funktionsfähig zu sein. Falls Knoten entfernt werden, so dass der Cluster nicht länger über ein Quorum verfügt, hängen sich Dienste und Speicher auf. Passen Sie entweder die erwarteten Stimmen an oder fügen Sie dem Cluster wieder die benötigte Anzahl an Knoten hinzu.



Anmerkung

Sie können einen Knoten manuell mit dem **`fence_node`** Befehl oder mit **Conga** abgrenzen. Für Informationen diesbezüglich, siehe **`fence_node`** Handbuchseite und Abschnitt 4.3.2, „Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen“.

9.6. Cluster-Dienst startet nicht

Falls ein vom Cluster verwalteter Dienst nicht startet, überprüfen Sie, ob die folgenden Gegebenheiten vorliegen:

- Die Dienstkonfiguration in der **`cluster.conf`** Datei enthält unter Umständen Syntaxfehler. Führen Sie den **`rg_test`** Befehl aus, um die Syntax in Ihrer Konfiguration zu überprüfen. Falls diese Konfigurations- oder Syntaxfehler enthält, wird **`rg_test`** Sie über das Problem informieren.

```
$ rg_test test /etc/cluster/cluster.conf start service servicename
```

  Für weitere Informationen über den **`rg_test`** Befehl, siehe Abschnitt C.5, „Testen und Fehlerbehebung von Diensten und der Ressourcenreihenfolge“.

  Ist die Konfiguration gültig, erhöhen Sie als Nächstes die Protokollierung des Ressourcengruppen-Managers und untersuchen die Protokolle, um Hinweise darauf zu erhalten, warum der Dienst nicht startet. Sie können die Protokollierungsstufe erhöhen, indem Sie den Parameter **`loglevel="7"`** zum **`rm`** Tag in der **`cluster.conf`** Datei hinzufügen. Dadurch erhalten Sie ausführlichere Protokollmeldungen hinsichtlich dem Starten, Stoppen und Migrieren von geclusterten Diensten.

9.7. Migration von Cluster-verwalteten Diensten schlägt fehl

Falls die Migration eines vom Cluster verwalteten Dienstes auf einen anderen Knoten fehlschlägt, der Dienst jedoch auf einem bestimmten Knoten startet, überprüfen Sie, ob die folgenden Gegebenheiten vorliegen:

- Vergewissern Sie sich, dass die Ressourcen, die zum Ausführen eines bestimmten Dienstes notwendig sind, auf allen Knoten im Cluster vorhanden sind, die unter Umständen diesen Dienst ausführen müssen. Falls Ihr geclusterter Dienst beispielsweise eine Skriptdatei an einem bestimmten Speicherort voraussetzt oder ein Dateisystem an einem bestimmten Einhängepunkt erwartet, dann müssen Sie sicherstellen, dass diese Ressourcen auf allen Knoten im Cluster an den erwarteten Orten vorliegen.
- Vergewissern Sie sich, dass Ausfallsicherungs-Domains, Dienstabhängigkeiten und Dienstexklusivität nicht derart konfiguriert sind, dass infolgedessen eine Migration von Diensten auf Knoten nicht erwartungsgemäß funktionieren kann.
- Falls es sich bei dem fraglichen Dienst um eine virtuelle Maschinenressource handelt, prüfen Sie die Dokumentation um sicherzustellen, dass Sie alle notwendigen Konfigurationen korrekt

vorgenommen haben.

- Erhöhen Sie die Protokollierung des Ressourcengruppen-Managers wie in Abschnitt 9.6, „Cluster-Dienst startet nicht“ beschrieben, und untersuchen Sie die Protokolle, um Hinweise darauf zu erhalten, warum die Migration des Dienstes fehlschlägt.

9.8. Jeder Knoten in einem Zwei-Knoten-Cluster meldet den jeweils anderen Knoten als ausgefallen

Falls es sich bei Ihrem Cluster um einen Zwei-Knoten-Cluster handelt und jeder Knoten meldet, dass er läuft, der jeweils andere Knoten jedoch angeblich ausgefallen ist, dann deutet dies darauf hin, dass die beiden Knoten nicht über Multicast oder über das Cluster-Heartbeat-Netzwerk miteinander kommunizieren können. Dieser Zustand der Netzwerkaufspaltung wird "Split Brain" genannt. Um dies zu beheben, folgen Sie den Hinweisen in Abschnitt 9.2, „Cluster wird nicht gebildet“.

9.9. Knoten werden nach LUN-Pfadausfall abgegrenzt

Wenn ein oder mehrere Knoten in Ihrem Cluster abgegrenzt werden, wenn ein LUN-Pfadausfall auftritt, kann dies daran liegen, dass ein Quorumdatenträger über Multipathing-Speicher verwendet wird. Falls Sie einen Quorumdatenträger verwenden und dieser Quorumdatenträger über Multipathing-Speicher verwendet wird, dann vergewissern Sie sich, dass Sie sämtliche Zeitangaben und Timeouts korrekt eingestellt haben, um einen Pfadausfall tolerieren zu können.

9.10. Quorumdatenträger erscheint nicht als Cluster-Mitglied

Falls Sie Ihr System zur Verwendung eines Quorumdatenträgers konfiguriert haben, diese jedoch nicht als Mitglied im Cluster erscheint, überprüfen Sie, ob die folgenden Gegebenheiten vorliegen:

- Vergewissern Sie sich, dass Sie **`chkconfig on`** für den **`qdisk`** Dienst festgelegt haben.
- Vergewissern Sie sich, dass Sie den **`qdisk`** Dienst gestartet haben.
- Beachten Sie, dass es einige Minuten dauern kann, bis sich der Quorumdatenträger beim Cluster registriert hat. Dies ist normales und erwartetes Verhalten.

9.11. Ungewöhnliches Verhalten bei Ausfallsicherung

Ein häufig auftretendes Problem mit Cluster-Servern ist ungewöhnliches Verhalten bei der Ausfallsicherung. Dienste stoppen, wenn andere Dienste starten, oder Dienste starten nicht auf einem anderen Knoten. Die Ursache hierfür kann in den komplexen Systemen zur Ausfallsicherung liegen, bestehend aus Ausfallsicherungs-Domains, Dienstabhängigkeiten und Dienstexklusivitäten. Versuchen Sie, Ihre Dienst- oder Ausfallsicherungskonfiguration zu vereinfachen, und testen Sie dann, ob das Problem weiterhin besteht. Vermeiden Sie Features wie Dienstexklusivität und -abhängigkeiten, wenn Sie sich nicht absolut sicher sind, wie diese Features die Ausfallsicherung unter allen denkbaren Bedingungen beeinflussen.

9.12. Wahlloses Fencing

Falls Sie feststellen, dass ein Knoten wahllos abgegrenzt wird, überprüfen Sie, ob die folgenden Gegebenheiten vorliegen:

- Die Ursache für das Fencing ist *immer* ein Knoten, der die Kommunikation mit dem Rest des Clusters abgebrochen hat und keinen "Heartbeat" mehr überträgt.
- Jede Situation, die dazu führt, dass ein System innerhalb einer festgelegten Zeitspanne keinen Heartbeat überträgt, kann die Abgrenzung verursachen. Standardmäßig beträgt diese Zeitspanne 10 Sekunden. Sie können diese Zeitspanne festlegen, indem Sie den gewünschten Wert (in Millisekunden) an den Token-Parameter des Totem-Tags in der **`cluster.conf`** Datei hinzufügen (z.B. **`totem token="30000"`** für 30 Sekunden).

- Vergewissern Sie sich, dass das Netzwerk einwandfrei funktioniert.
- Stellen Sie sicher, dass die Schnittstellen, die der Cluster für die Kommunikation zwischen Knoten benutzt, nur Bindungs-Modus 0, 1 oder 2 verwenden. (Bindungs-Modus 0 und 2 werden ab Red Hat Enterprise Linux 6.4 unterstützt.)
- Führen Sie Maßnahmen durch, um festzustellen, ob das System sich aufhängt oder ob eine Kernel-Panik auftritt. Richten Sie das **kdump** Dienstprogramm ein, um einen Speicherauszug während einer dieser wahllosen Abgrenzungen zu erhalten.
- Stellen Sie sicher, dass Sie die auftretende Situation nicht fälschlicherweise für eine Abgrenzung halten, obwohl es ggf. zum Beispiel der Quorumdatenträger ist, die aufgrund eines Speicherausfalls einen Knoten ausschließt, oder ein Produkt eines Drittanbieters wie Oracle RAC, das einen Knoten aus anderen Gründen neu startet. Die Nachrichtenprotokolle sind oft hilfreich, um diese Probleme zu untersuchen. Bei jeder Abgrenzung oder jedem Knoten-Neustart sollten Sie standardmäßig die Nachrichtenprotokolle vom Zeitpunkt der Abgrenzung/des Neustarts auf allen Knoten im Cluster überprüfen.
- Überprüfen Sie das System zudem gründlich auf Hardware-Fehler, die dazu führen könnten, dass das System nicht erwartungsgemäß auf Heartbeats reagiert.

9.13. Debug-Protokollierung für Distributed Lock Manager (DLM) muss aktiviert sein

Es gibt zwei Debugging-Optionen für den Distributed Lock Manager (DLM), die Sie bei Bedarf aktivieren können: DLM-Kernel-Debugging und POSIX-Lock-Debugging.

Um DLM-Debugging zu aktivieren, bearbeiten Sie die **/etc/cluster/cluster.conf** Datei, um Konfigurationsoptionen zum **dlm** Tag hinzuzufügen. Die **log_debug** Option aktiviert DLM-Kernel-Debuggingnachrichten und die **plock_debug** Option aktiviert POSIX-Sperren-Debuggingnachrichten.

Der folgende Beispielabschnitt einer **/etc/cluster/cluster.conf** Datei zeigt den **dlm** Tag, der beide DLM-Debugoptionen aktiviert:

```
<cluster config_version="42" name="cluster1">
  ...
  <dlm log_debug="1" plock_debug="1"/>
  ...
</cluster>
```

Nachdem Sie die **/etc/cluster/cluster.conf** Datei bearbeitet haben, führen Sie den **cman_tool version -r** Befehl aus, um die Konfiguration an die übrigen Cluster-Knoten weiterzugeben.

Kapitel 10. SNMP-Konfiguration mit dem Red Hat Hochverfügbarkeits-Add-On

Ab der Red Hat Enterprise Linux 6.1 Release bietet das Red Hat Hochverfügbarkeits-Add-On Unterstützung für SNMP-Traps. Dieses Kapitel beschreibt, wie Sie Ihr System für SNMP konfigurieren können, gefolgt von einer Zusammenfassung der Traps, die das Red Hat Hochverfügbarkeits-Add-On für bestimmte Cluster-Ereignisse ausgibt.

10.1. SNMP und das Red Hat Hochverfügbarkeits-Add-On

Der Red Hat Hochverfügbarkeits-Add-On SNMP-Subagent ist **foghorn**, der die SNMP-Traps ausgibt. Der **foghorn** Subagent kommuniziert mit dem **snmpd** Daemon über das AgentX-Protokoll. Der **foghorn** Subagent erstellt lediglich SNMP-Traps; er unterstützt keine anderen SNMP-Operationen wie z.B. **get** oder **set**.

Es gibt derzeit keine **config** Optionen für den **foghorn** Subagent. Er kann nicht zur Verwendung eines bestimmten Sockets konfiguriert werden; nur der standardmäßige AgentX-Socket wird derzeit unterstützt.

10.2. Konfiguration von SNMP mit dem Red Hat Hochverfügbarkeits-Add-On

Um SNMP für das Red Hat Hochverfügbarkeits-Add-On zu konfigurieren, führen Sie die folgenden Schritte auf jedem Knoten im Cluster aus, um sicherzustellen, dass die nötigen Dienste aktiviert sind und ausgeführt werden.

1. Um SNMP-Traps mit dem Red Hat Hochverfügbarkeits-Add-On zu verwenden, ist der **snmpd** Dienst erforderlich, der als Master-Agent fungiert. Da der **foghorn** Dienst der Subagent ist und das AgentX-Protokoll verwendet, müssen Sie die folgende Zeile zur **/etc/snmp/snmpd.conf** Datei hinzufügen, um AgentX-Unterstützung zu aktivieren:

```
master agentx
```

2. Um den Host festzulegen, an den die SNMP-Trap-Benachrichtigungen gesendet werden sollen, fügen Sie die folgende Zeile zur **/etc/snmp/snmpd.conf** Datei hinzu:

```
trap2sink host
```

   Weitere Informationen über die Handhabung der Benachrichtigungen finden Sie auf der **snmpd.conf** Handbuchseite.

3. Vergewissern Sie sich, dass der **snmpd** Daemon aktiviert ist und läuft, indem Sie die folgenden Befehle ausführen:

```
# chkconfig snmpd on
# service snmpd start
```

4. Falls der **messagebus** Daemon noch nicht aktiviert ist und noch nicht läuft, führen Sie die folgenden Befehle aus:

```
# chkconfig messagebus on
# service messagebus start
```

5. Vergewissern Sie sich, dass der **foghorn** Daemon aktiviert ist und läuft, indem Sie die folgenden Befehle ausführen:

```
# chkconfig foghorn on
# service foghorn start
```

6. Führen Sie den folgenden Befehl aus, um Ihr System so zu konfigurieren, dass der **COROSYNC-MIB** SNMP-Traps generiert und um sicherzustellen, dass der **corosync-notifyd** Daemon aktiviert ist und läuft:

```
# echo "OPTIONS=\"-d\" " > /etc/sysconfig/corosync-notifyd
# chkconfig corosync-notifyd on
# service corosync-notifyd start
```

Nachdem Sie jeden Knoten im Cluster für SNMP konfiguriert haben und sichergestellt haben, dass die nötigen Dienste laufen, werden D-bus Signale nunmehr vom **foghorn** Dienst empfangen und in SNMPv2-Traps übersetzt. Diese Traps werden anschließend an den Host übertragen, den Sie mit dem **trapsink** Eintrag zum Empfang von SNMPv2-Traps definiert haben.

10.3. Weiterleiten von SNMP-Traps

Es ist möglich, SNMP-Traps an einen Rechner außerhalb des Clusters weiterzuleiten, auf der Sie den **snmptrapd** Daemon einsetzen und anpassen können, wie die Benachrichtigungen gehandhabt werden sollen.

Um SNMP-Traps in einem Cluster auf einen Rechner außerhalb des Clusters weiterzuleiten, führen Sie die folgenden Schritte aus:

1. Folgen Sie für jeden Knoten im Cluster dem in Abschnitt 10.2, „Konfiguration von SNMP mit dem Red Hat Hochverfügbarkeits-Add-On“ beschriebenen Verfahren, und geben Sie dabei im **trap2sink *host*** Eintrag in der **/etc/snmp/snmpd.conf** Datei den externen Host an, auf dem der **snmptrapd** Daemon ausgeführt werden soll.
2. Bearbeiten Sie auf dem externen Host, der die Traps empfangen wird, die **/etc/snmp/snmptrapd.conf** Konfigurationsdatei, um Ihre Community-Strings festzulegen. Beispielsweise können Sie den folgenden Eintrag verwenden, um es dem **snmptrapd** Daemon zu ermöglichen, Benachrichtigungen unter Verwendung des **public** Community-Strings zu verarbeiten.

```
authCommunity log,execute,net public
```

3. Vergewissern Sie sich auf dem externen Host, der die Traps empfangen wird, dass der **snmptrapd** Daemon aktiviert ist und läuft, indem Sie die folgenden Befehle ausführen:

```
# chkconfig snmptrapd on
# service snmptrapd start
```

Für weitere Informationen über die Verarbeitung von SNMP-Benachrichtigungen siehe die **snmptrapd.conf** Handbuchseite.

10.4. SNMP-Traps generiert vom Red Hat Hochverfügbarkeits-Add-On

Der **foghorn** Daemon generiert die folgenden Traps:

- **fenceNotifyFenceNode**

  Diese Trap tritt auf, wenn ein abgegrenzter Knoten versucht, einen anderen Knoten abzugrenzen. Beachten Sie, dass diese Trap nur auf einem Knoten generiert wird - auf demjenigen Knoten, der die Fencing-Operation durchzuführen versucht. Die Benachrichtigung beinhaltet die folgenden Felder:

  - **fenceNodeName** - Name des abgegrenzten Knotens

  - **fenceNodeID** - Knoten-ID des abgegrenzten Knotens
  - **fenceResult** - das Ergebnis der Fencing-Operation (0 falls erfolgreich, -1 falls Fehler auftraten, -2 falls keine Fencing-Methoden definiert sind)

- **rgmanagerServiceStateChange**

  Diese Trap tritt auf, wenn sich der Status eines Cluster-Dienstes ändert. Die Benachrichtigung beinhaltet die folgenden Felder:

  - **rgmanagerServiceName** - der Name des Dienstes einschließlich Diensttyp (z.B. **service:foo** oder **vm:foo**).
  - **rgmanagerServiceState** - der Status des Dienstes. Davon ausgenommen sind Übergangszustände wie **starting** und **stopping**, um die Traps übersichtlich zu halten.
  - **rgmanagerServiceFlags** - die Dienst-Flags. Derzeit gibt es zwei unterstützte Flags: **frozen**, was einen Dienst kennzeichnet, der mithilfe des Befehls **clusvcadm -Z** eingefroren wurde, und **partial**, was einen Dienst kennzeichnet, in dem eine ausgefallene Ressource als **non-critical** markiert wurde, so dass die Ressource ausfallen und deren Komponenten manuell neu gestartet werden können, ohne dass der gesamte Dienst davon betroffen ist.
  - **rgmanagerServiceCurrentOwner** - der Dienstbesitzer. Falls der Dienst nicht läuft, ist dies **(none)**.
  - **rgmanagerServicePreviousOwner** - der letzte Dienstbesitzer, sofern bekannt. Ist der letzte Dienstbesitzer nicht bekannt, ist dies ggf. **(none)**.

Der **corosync-nodifyd** Daemon generiert die folgenden Traps:

- **corosyncNoticesNodeStatus**

  Diese Trap tritt auf, wenn ein Knoten einem Cluster beitritt oder diesen verlässt. Die Benachrichtigung beinhaltet die folgenden Felder:

  - **corosyncObjectsNodeName** - Knotenname
  - **corosyncObjectsNodeID** - Knoten-ID
  - **corosyncObjectsNodeAddress** - Knoten-IP-Adresse
  - **corosyncObjectsNodeStatus** - Knotenstatus (**joined** oder **left**)

- **corosyncNoticesQuorumStatus**

  Diese Trap tritt auf, wenn sich der Quorumstatus ändert. Die Benachrichtigung beinhaltet die folgenden Felder:

  - **corosyncObjectsNodeName** - Knotenname
  - **corosyncObjectsNodeID** - Knoten-ID
  - **corosyncObjectsQuorumStatus** - neuer Status des Quorum (**quorate** oder **NOT quorate**)

- **corosyncNoticesAppStatus**

  Diese Trap tritt auf, wenn eine Client-Applikation eine Verbindung mit Corosync herstellt oder diese unterbricht.

  - **corosyncObjectsNodeName** - Knotenname
  - **corosyncObjectsNodeID** - Knoten-ID
  - **corosyncObjectsAppName** - Applikationsname
  - **corosyncObjectsAppStatus** - neuer Status einer Applikation (**connected** oder **disconnected**)

Kapitel 11. Konfiguration von geclustertem Samba

Ab der Red Hat Enterprise Linux 6.2 Release bietet die Red Hat Hochverfügbarkeits-Add-On Unterstützung für die Ausführung von geclustertem Samba in einer Aktiv/Aktiv-Konfiguration. Dies erfordert, dass Sie CTDB auf allen Knoten in einem Cluster, die Sie in Verbindung mit GFS2 Cluster-Dateisystemen verwenden, installieren und konfigurieren.



Anmerkung

Red Hat Enterprise Linux 6 unterstützt bis zu vier Knoten, auf denen geclustertes Samba ausgeführt wird.

Dieses Kapitel beschreibt das Verfahren zur Konfiguration von CTDB anhand der Konfiguration eines Beispielsystems. Informationen über die Konfiguration von GFS2-Dateisystemen finden Sie im Handbuch *Global File System 2*. Informationen über die Konfiguration logischer Datenträger finden Sie im Handbuch *Administration des Logical Volume Manager*.



Anmerkung

Ein zeitgleicher Zugriff von außerhalb Sambas auf die Daten auf der Samba-Freigabe wird nicht unterstützt.

11.1. Überblick über CTDB

CTDB ist eine Cluster-Implementierung der TDB-Datenbank von Samba. Um CTDB zu verwenden, muss auf allen Knoten im Cluster ein geclustertes Dateisystem verfügbar und freigegeben sein. CTDB liefert die geclusterten Features aufbauend auf diesem geclusterten Dateisystem. Seit der Red Hat Enterprise Linux 6.2 Release führt CTDB auch einen Cluster-Stack parallel zu dem von Red Hat Enterprise Linux Clustering. CTDB steuert Knotenmitgliedschaft, Wiederherstellung/Ausfallsicherheit, IP Relocation und Samba-Dienste.

11.2. Erforderliche Pakete

Zusätzlich zu den Standardpaketen, die zur Ausführung des Red Hat Hochverfügbarkeits-Add-Ons und des Red Hat Resilient Storage Add-Ons nötig sind, erfordert der Einsatz von Samba mit Red Hat Enterprise Linux Clustering die folgenden Pakete:

- **`ctdb`**
- **`samba`**
- **`samba-common`**
- **`samba-winbind-clients`**

11.3. GFS2-Konfiguration

Die Konfiguration von Samba mit Red Hat Enterprise Linux Clustering erfordert zwei GFS2-Dateisysteme: Ein kleines Dateisystem für CTDB und ein zweites Dateisystem für die Samba-Freigabe. Dieses Beispiel veranschaulicht, wie diese beiden GFS2-Dateisysteme erstellt werden.

Bevor Sie die GFS2-Dateisysteme erstellen, müssen Sie zunächst einen logischen LVM-Datenträger für jedes der Dateisysteme erstellen. Informationen über das Anlegen von logischen LVM-Datenträgern finden Sie im Handbuch *Administration des Logical Volume Manager*. Dieses Beispiel verwendet die folgenden logischen Datenträger:

- **/dev/csmb_vg/csmb_lv**, auf dem die Benutzerdaten enthalten sind, die über die Samba-Freigabe exportiert werden, und der dementsprechend groß sein sollte. Dieses Beispiel erstellt einen logischen Datenträger, der 100 GB groß ist.
- **/dev/csmb_vg/ctdb_lv**, auf dem die gemeinsam verwendeten CTDB-Zustandsinformationen gespeichert werden. Dieser Datenträger muss 1 GB groß sein.

Erstellen Sie die geclusterten Datenträgergruppen und logischen Datenträger nur auf einem einzigen Knoten im Cluster.

Um ein GFS2-Dateisystem auf einem logischen Datenträger zu erstellen, führen Sie den **mkfs.gfs2** Befehl aus. Führen Sie diesen Befehl nur auf einem einzigen Knoten im Cluster aus.

Um auf dem logischen Datenträger **/dev/csmb_vg/csmb_lv** das Dateisystem zu erstellen, das die Samba-Freigabe beherbert, führen Sie den folgenden Befehl aus:

```
[root@clusmb-01 ~]# mkfs.gfs2 -j3 -p lock_dlm -t csmb:gfs2 /dev/csmb_vg/csmb_lv
```

Die Parameter bedeuten:

-j
: Spezifiziert die Anzahl der Journale, die im Dateisystem erstellt werden sollen. Dieses Beispiel erstellt einen Cluster mit drei Knoten, wir erstellen also ein Journal pro Knoten.

-p
: Spezifiziert das Sperrprotokoll. **lock_dlm** ist das Sperrprotokoll, das GFS2 für die Kommunikation der Knoten untereinander verwendet.

-t
: Spezifiziert den Namen der Sperrtabelle und folgt dem Format ***cluster_name:fs_name***. In diesem Beispiel lautet der in der **cluster.conf** Datei festgelegte Cluster-Name **csmb** und wir verwenden **gfs2** als Namen für das Dateisystem.

Die Ausgabe dieses Befehls sieht wie folgt aus:

```
This will destroy any data on /dev/csmb_vg/csmb_lv.
  It appears to contain a gfs2 filesystem.

Are you sure you want to proceed? [y/n] y

Device:
/dev/csmb_vg/csmb_lv
Blocksize:  4096
Device Size  100.00 GB (26214400 blocks)
Filesystem Size: 100.00 GB (26214398 blocks)
Journals:  3
Resource Groups:  400
Locking Protocol:   "lock_dlm"
Lock Table:   "csmb:gfs2"
UUID:
  94297529-ABG3-7285-4B19-182F4F2DF2D7
```

In diesem Beispiel wird das **/dev/csmb_vg/csmb_lv** Dateisystem auf allen Knoten unter **/mnt/gfs2** eingehängt. Dieser Einhängepunkt muss dem Wert entsprechen, den Sie als Speicherort des **share** Verzeichnisses mit der **path =** Option in der **/etc/samba/smb.conf** Datei angeben, wie in Abschnitt 11.5, „Samba-Konfiguration“ beschrieben.

Um auf dem logischen Datenträger **/dev/csmb_vg/ctdb_lv** das Dateisystem zu erstellen, das die CTDB-Zustandsinformationen beherbert, führen Sie den folgenden Befehl aus:

```
[root@clusmb-01 ~]# mkfs.gfs2 -j3 -p lock_dlm -t csmb:ctdb_state
/dev/csmb_vg/ctdb_lv
```

Beachten Sie, dass dieser Befehl einen anderen Sperrtabellennamen spezifiziert, als der Befehl zum Erstellen des Dateisystems auf **/dev/csmb_vg/csmb_lv**. Dadurch unterscheiden sich die Sperrtabellennamen für die verschiedenen Geräte, die für die Dateisysteme verwendet werden.

Die Ausgabe des **mkfs.gfs2** Befehl sieht wie folgt aus:

```
This will destroy any data on /dev/csmb_vg/ctdb_lv.
  It appears to contain a gfs2 filesystem.

Are you sure you want to proceed? [y/n] y

Device:
/dev/csmb_vg/ctdb_lv
Blocksize:    4096
Device Size   1.00 GB (262144 blocks)
Filesystem Size:  1.00 GB (262142 blocks)
Journals:  3
Resource Groups:  4
Locking Protocol:  "lock_dlm"
Lock Table:   "csmb:ctdb_state"
UUID:
  BCDA8025-CAF3-85BB-B062-CC0AB8849A03
```

In diesem Beispiel wird das **/dev/csmb_vg/ctdb_lv** Dateisystem auf allen Knoten unter **/mnt/ctdb** eingehängt. Dieser Einhängepunkt muss dem Wert entsprechen, den Sie als Speicherort der **.ctdb.lock** Datei mit der **CTDB_RECOVERY_LOCK** Option in der **/etc/sysconfig/ctdb** Datei angeben, wie in Abschnitt 11.4, „CTDB-Konfigurationen“ beschrieben.

11.4. CTDB-Konfigurationen

Die CTDB Konfigurationsdatei befindet sich unter **/etc/sysconfig/ctdb**. Die folgenden Felder sind für die CTDB-Konfiguration erforderlich:

- **CTDB_NODES**
- **CTDB_PUBLIC_ADDRESSES**
- **CTDB_RECOVERY_LOCK**
- **CTDB_MANAGES_SAMBA** (muss aktiviert sein)
- **CTDB_MANAGES_WINBIND** (muss aktiviert sein, falls auf einem Mitgliedsserver ausgeführt)

Das folgende Beispiel zeigt eine Konfigurationsdatei, in der Beispielparameter für die Felder angegeben wurden, die für den Einsatz von CTDB erforderlich sind:

```
CTDB_NODES=/etc/ctdb/nodes
CTDB_PUBLIC_ADDRESSES=/etc/ctdb/public_addresses
CTDB_RECOVERY_LOCK="/mnt/ctdb/.ctdb.lock"
CTDB_MANAGES_SAMBA=yes
CTDB_MANAGES_WINBIND=yes
```

Die Parameter bedeuten:

CTDB_NODES

Spezifiziert den Speicherort der Datei mit der Cluster-Knotenliste.

Die **/etc/ctdb/nodes** Datei, auf die **CTDB_NODES** verweist, listet einfach die IP-Adressen der Cluster-Knoten, wie im folgenden Beispiel veranschaulicht:

```
192.168.1.151
192.168.1.152
192.168.1.153
```

In diesem Beispiel gibt es nur eine Schnittstelle/IP auf jedem Knoten, die sowohl zur Cluster/CTDB-Kommunikation als auch zur Handhabung von Client-Anfragen verwendet wird. Allerdings empfehlen wir dringend Cluster-Knoten mit zwei Netzwerkschnittstellen, so dass eine Schnittstellengruppe der Cluster/CTDB-Kommunikation und eine andere dem öffentlichen Client-Zugriff dienen kann. Verwenden Sie hier entsprechenden IP-Adressen des Cluster-Netzwerks und achten Sie darauf, dass die Hostnamen bzw. IP-Adressen in der **cluster.conf** Datei damit übereinstimmen. Verwenden Sie ebenso die entsprechenden Schnittstellen des öffentlichen Netzwerks für den Client-Zugriff in der **public_addresses** Datei.

Es ist von entscheidender Bedeutung, dass die **/etc/ctdb/nodes** Datei auf allen Knoten identisch ist, denn die Reihenfolge der Einträge ist wichtig und CTDB würde fehlschlagen, falls auf verschiedenen Knoten abweichende Informationen vorliegen.

CTDB_PUBLIC_ADDRESSES

Spezifiziert den Speicherort der Datei, in der IP-Adressen aufgeführt sind, die zum Zugriff auf die vom Cluster exportierten Samba-Freigaben genutzt werden können. Dies sind die IP-Adressen, die Sie in DNS für den Namen des geclusterten Samba-Servers konfigurieren sollten und mit denen sich CIFS-Clients verbinden werden. Konfigurieren Sie den Namen des geclusterten Samba-Servers als einen DNS-Typ-A-Eintrag mit mehreren IP-Adressen und lassen Sie DNS die Clients reihum ("Round Robin") an die Knoten im Cluster verteilen.

Für dieses Beispiel haben wir einen Round-Robin DNS-Eintrag **csmb-server** konfiguriert mit allen Adressen, die in der **/etc/ctdb/public_addresses** Datei aufgeführt sind. DNS verteilt die Clients, die diesen Eintrag nutzen, reihum an die Knoten im Cluster.

Die **/etc/ctdb/public_addresses** Datei auf jedem Knoten hat den folgenden Inhalt:

```
192.168.1.201/0 eth0
192.168.1.202/0 eth0
192.168.1.203/0 eth0
```

Dieses Beispiel verwendet drei Adressen, die derzeit nicht im Netzwerk verwendet werden. Wählen Sie für Ihre eigene Konfiguration Adressen, auf die von den zukünftigen Clients zugegriffen werden kann.

Alternativ zeigt das folgende Beispiel die Inhalte der **/etc/ctdb/public_addresses** Dateien in einem Cluster, der drei Knoten umfasst, jedoch insgesamt vier öffentliche Adressen hat. In diesem Beispiel kann die IP-Adresse 198.162.2.1 entweder von Knoten 0 oder Knoten 1 gehostet werden und wird für Clients verfügbar sein, solange mindestens einer dieser beiden Knoten verfügbar ist. Nur wenn Knoten 0 und 1 beide ausfallen, ist diese öffentliche Adresse für Clients nicht länger verfügbar. Alle anderen öffentlichen Adressen können jeweils von nur einem einzigen Knoten bedient werden und sind somit nur dann verfügbar, wenn auch der jeweilige Knoten verfügbar ist.

Die **/etc/ctdb/public_addresses** Datei auf Knoten 0 hat den folgenden Inhalt:

```
198.162.1.1/24 eth0
198.162.2.1/24 eth1
```

Die **/etc/ctdb/public_addresses** Datei auf Knoten 1 hat den folgenden Inhalt:

```
198.162.2.1/24 eth1
198.162.3.1/24 eth2
```

Die **/etc/ctdb/public_addresses** Datei auf Knoten 2 hat den folgenden Inhalt:

```
198.162.3.2/24 eth2
```

CTDB_RECOVERY_LOCK

Spezifiziert eine Sperrdatei, die CTDB intern zur Wiederherstellung benutzt. Diese Datei muss sich auf gemeinsam verwendetem Speicher befinden, damit alle Cluster-Knoten darauf zugreifen können. Das Beispiel in diesem Abschnitt benutzt ein GFS2-Dateisystem, das auf allen Knoten unter **/mnt/ctdb** eingehängt wird. Es unterscheidet sich von jenem GFS2-Dateisystem, das die zu exportierende Samba-Freigabe enthält. Diese Sperrdatei zur Wiederherstellung wird verwendet, um eine Aufspaltung des Clusters ("Split-Brain") zu verhindern. Unter neueren Versionen von CTDB (1.0.112 und höher) ist die Angabe dieser Datei optional, vorausgesetzt, es wird ein anderer Mechanismus verwendet, der Cluster-Aufspaltungen verhindert.

CTDB_MANAGES_SAMBA

Falls durch die Einstellung **yes** aktiviert, darf CTDB den Samba-Dienst nach eigenem Ermessen starten und stoppen, um Dienstmigration/Ausfallsicherung zur Verfügung zu stellen.

Wenn **CTDB_MANAGES_SAMBA** aktiviert ist, sollten Sie den automatischen **init** Start der **smb** und **nmb** Daemons mithilfe der folgenden Befehle deaktivieren:

```
[root@clusmb-01 ~]# chkconfig snb off
[root@clusmb-01 ~]# chkconfig nmb off
```

CTDB_MANAGES_WINBIND

Falls durch die Einstellung **yes** aktiviert, darf CTDB den **winbind** Daemon nach eigenem Ermessen starten und stoppen. Dies sollte aktiviert werden, wenn Sie CTDB in einer Windows-Domain oder im Active Directory Security-Modus verwenden.

Wenn **CTDB_MANAGES_WINBIND** aktiviert ist, sollten Sie den automatischen **init** Start des **winbind** Daemons mithilfe des folgenden Befehls deaktivieren:

```
[root@clusmb-01 ~]# chkconfig windinbd off
```

11.5. Samba-Konfiguration

Die Samba-Konfigurationsdatei **smb.conf** befindet sich in diesem Beispiel unter **/etc/samba/smb.conf**. Sie enthält die folgenden Parameter:

```
[global]
 guest ok = yes
 clustering = yes
 netbios name = csmb-server
[csmb]
 comment = Clustered Samba
  public = yes
 path = /mnt/gfs2/share
 writeable = yes
 ea support = yes
```

Dieses Beispiel exportiert eine Freigabe namens **csmb** unter **/mnt/gfs2/share**. Sie unterscheidet sich vom gemeinsam verwendeten GFS2-Dateisystem unter **/mnt/ctdb/.ctdb.lock**, das wir als **CTDB_RECOVERY_LOCK** Parameter in der CTDB-Konfigurationsdatei unter **/etc/sysconfig/ctdb** spezifiziert haben.

In diesem Beispiel erstellen wir das **share** Verzeichnis in **/mnt/gfs2**, wenn wir es zum ersten Mal einhängen. Der **clustering = yes** Eintrag weist Samba zur Verwendung von CTDB an. Der **netbios name = csmb-server** Eintrag richtet alle Knoten explizit mit demselben NetBIOS-Namen ein. Der **ea support** Parameter ist erforderlich, falls Sie erweiterte Parameter nutzen möchten.

Die **cluster.conf** Konfigurationsdatei muss auf allen Cluster-Knoten identisch sein.

Samba bietet auch Registry-basierte Konfiguration mithilfe des **net conf** Befehls, um die Konfiguration automatisch auf allen Cluster-Mitgliedern synchron zu halten, ohne manuell die Konfigurationsdateien zwischen den Cluster-Knoten hin- und herkopieren zu müssen. Weitere Informationen über den **net conf** Befehl finden Sie auf der **net**(8) Handbuchseite.

11.6. Starten von CTDB und Samba-Diensten

Nach dem Start des Clusters müssen Sie die GFS2-Dateisysteme einhängen, die Sie wie in Abschnitt 11.3, „GFS2-Konfiguration“ beschrieben erstellt haben. Die Berechtigungen auf dem Samba **share** Verzeichnis und den Benutzerkonten auf den Cluster-Knoten sollten für den Client-Zugriff eingerichtet sein.

Führen Sie den folgenden Befehl auf allen Knoten aus, um den **ctdbd** Daemon zu starten. Da dieses Beispiel CTDB mit **CTDB_MANAGES_SAMBA=yes** konfiguriert hat, wird CTDB auch die Samba-Dienste auf allen Knoten starten und alle konfigurierten Samba-Freigaben exportieren.

```
[root@clusmb-01 ~]# service ctdb start
```

Es kann einige Minuten dauern, bis CTDB Samba gestartet und die Freigaben exportiert hat. Führen Sie **ctdb status** aus, um den Status von CTDB anzusehen, wie das folgende Beispiel veranschaulicht:

```
[root@clusmb-01 ~]# ctdb status
Number of nodes:3
pnn:0 192.168.1.151     OK (THIS NODE)
pnn:1 192.168.1.152     OK
pnn:2 192.168.1.153     OK
Generation:1410259202
Size:3
hash:0 lmaster:0
hash:1 lmaster:1
hash:2 lmaster:2
Recovery mode:NORMAL (0)
Recovery master:0
```

Wenn Sie sehen, dass alle Knoten den Vermerk "OK" tragen, können Sie damit fortfahren, den geclusterten Samba-Server zu verwenden, wie in Abschnitt 11.7, „Verwenden des geclusterten Samba-

Servers“ beschrieben.

11.7. Verwenden des geclusterten Samba-Servers

Clients können sich mit der exportierten Samba-Freigabe verbinden, indem Sie sich mit einer der IP-Adressen verbinden, die in der **/etc/ctdb/public_addresses** Datei festgelegt wurden, oder indem Sie den **csmb-server** DNS-Eintrag nutzen, der in einem früheren Schritt konfiguriert wurde:

```
[root@clusmb-01 ~]# mount -t cifs //csmb-server/csmb /mnt/sambashare -o
user=testmonkey
```

oder

```
[user@clusmb-01 ~]$ smbclient //csmb-server/csmb
```

Parameter der Fencing-Geräte

Dieser Anhang enthält Tabellen mit Parameterbeschreibungen für Fencing-Geräte. Sie können diese Parameter mithilfe von **luci** oder unter Verwendung des **ccs** Befehls konfigurieren, oder indem Sie die **etc/cluster/cluster.conf** Datei bearbeiten. Eine vollständige Liste der Fencing-Geräteparameter samt Beschreibungen finden Sie auf der Handbuchseite des jeweiligen Agenten.



Anmerkung

Der **Name** Parameter für ein Fencing-Gerät spezifiziert für das Gerät einen beliebigen Namen, der vom Red Hat Hochverfügbarkeits-Add-On verwendet wird. Es handelt sich hierbei nicht um den DNS-Namen für das Gerät.



Anmerkung

Bestimmte Fencing-Geräte haben einen optionalen **Password Script** Parameter. Mithilfe des **Password Script** Parameters können Sie festlegen, dass ein Fencing-Gerätepasswort von einem Skript zur Verfügung gestellt wird, anstatt vom **Password** Parameter. Die Verwendung des **Password Script** Parameters ersetzt den **Password** Parameter und ermöglicht, dass Passwörter in der Cluster-Konfigurationsdatei (**/etc/cluster/cluster.conf**) nicht sichtbar sind.

Tabelle A.1, „Übersicht über Fencing-Geräte“ listet die Fencing-Geräte und die damit verknüpften Fencing-Geräte-Agenten, und liefert einen Verweis auf die Tabelle, in der die Parameter für die Fencing-Geräte dokumentiert sind.

Tabelle A.1. Übersicht über Fencing-Geräte

Fencing-Gerät	Fencing-Agent	Verweis auf Parameterbeschreibung
APC Power Switch (telnet/SSH)	fence_apc	Tabelle A.2, „APC Power Switch (telnet/SSH)“
APC Power Switch über SNMP	fence_apc_snmp	Tabelle A.3, „APC Power Switch über SNMP“
Brocade Fabric Switch	fence_brocade	Tabelle A.4, „Brocade Fabric Switch“
Cisco MDS	fence_cisco_mds	Tabelle A.5, „Cisco MDS“
Cisco UCS	fence_cisco_ucs	Tabelle A.6, „Cisco UCS“
Dell DRAC 5	fence_drac5	Tabelle A.7, „Dell DRAC 5“
Eaton Netzwerk Stromversorgungs-Schalter (SNMP Schnittstelle)	fence_eaton_snmp	Tabelle A.8, „Eaton Netzwerk Stromversorgungs-Schalter Steuerung (SNMP Schnittstelle) (Red Hat Enterprise Linux 6.4 und höher)“
Egenera SAN-Controller	fence_egenera	Tabelle A.9, „Egenera SAN-Controller“
ePowerSwitch	fence_eps	Tabelle A.10, „ePowerSwitch“
Fence virt	fence_virt	Tabelle A.11, „Fence virt“
Fujitsu Siemens Remoteview Service Board (RSB)	fence_rsb	Tabelle A.12, „Fujitsu Siemens Remoteview Service Board (RSB)“
HP BladeSystem	fence_hpblade	Tabelle A.13, „HP BladeSystem (Red Hat Enterprise Linux 6.4 und höher)“
HP iLO (Integrated Lights Out), HP iLO2	fence_ilo, fence_ilo2	Tabelle A.14, „HP iLO (Integrated Lights Out) und HP iLO2“
HP iLO (Integrated Lights Out) MP	fence_ilo_mp	Tabelle A.15, „HP iLO (Integrated Lights Out) MP“
IBM BladeCenter	fence_bladecenter	Tabelle A.16, „IBM BladeCenter“
IBM BladeCenter SNMP	fence_ibmblade	Tabelle A.17, „IBM BladeCenter SNMP“
IBM iPDU	fence_ipdu	Tabelle A.18, „IBM iPDU (Red Hat Enterprise Linux 6.4 und höher)“
IF MIB	fence_ifmib	Tabelle A.19, „IF MIB“
Intel Modular	fence_intelmodular	Tabelle A.20, „Intel Modular“
IPMI (Intelligent Platform Management	fence_ipmilan, fence_imm, fence_idrac, fence_ilo3, fence_ilo4	Tabelle A.21, „IPMI (Intelligent Platform Management Interface) LAN, Dell iDrac, IBM Integriertes

Interface) LAN, IBM Integriertes Managementmodul, Dell iDRAC, HPiLO3, HPiLO4.		Managementmodul, HPiLO3, HPiLO4“
RHEV-M REST-API	fence_rhevm	Tabelle A.22, „RHEV-M REST API (RHEL 6.2 und höher mit RHEV 3.0 und höher)“
SCSI-Fencing	fence_scsi	Tabelle A.23, „SCSI Reservation Fencing“
VMware-Fencing (SOAP-Schnittstelle)	fence_vmware_soap	Tabelle A.24, „VMware Fencing (SOAP-Schnittstelle) (Red Hat Enterprise Linux 6.2 und höher)“
WTI Power Switch	fence_wti	Tabelle A.25, „WTI Power Switch“

Tabelle A.2, „APC Power Switch (telnet/SSH)“ listet die Fencing-Geräteparameter, die von **`fence_apc`** - dem Fencing-Agenten für APC über Telnet/SSH - verwendet werden.

Tabelle A.2. APC Power Switch (telnet/SSH)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das mit dem Cluster verbundene APC-Gerät, bei dem sich der Fencing-Daemon über telnet/ssh anmeldet.
IP Address or Hostname	**ipaddr**	Die IP-Adresse oder der Hostname des Geräts.
IP-Port (optional)	**ipport**	Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port.
Login	**login**	Der Login-Name für den Zugriff auf das Gerät.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
Power Wait (seconds)	**power_wait**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	**power_timeout**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	**shell_timeout**	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	**login_timeout**	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	**retry_on**	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Port	**port**	Der Port.
Switch (optional)	**switch**	Die Switch-Nummer für den APC-Switch, der mit dem Knoten verbindet, wenn Sie mehrere in Reihe geschaltete Switches haben.
Delay (optional)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.
Use SSH	**secure**	Zeigt an, dass das System SSH zum Zugriff auf das Gerät verwendet. Bei der Verwendung von SSH müssen Sie entweder ein Passwort, ein Passwortskript oder eine Identitätsdatei angeben.
Path to SSH Identity File	**identity_file**	Die Identitätsdatei für SSH.

Tabelle A.3, „APC Power Switch über SNMP“ listet die Fencing-Geräteparameter, die von **fence_apc_snmp** - dem Fencing-Agenten für APC, der sich direkt über das SNMP-Protokoll bei dem SNP-Gerät anmeldet - verwendet werden.

Tabelle A.3. APC Power Switch über SNMP

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das mit dem Cluster verbundene APC-Gerät, bei dem sich der Fencing-Daemon über das SNMP-Protokoll anmeldet.
IP Address or Hostname	**ipaddr**	Die IP-Adresse oder der Hostname des Geräts.
UDP/TCP port	**udpport**	Der zur Verbindung mit diesem Gerät zu verwendende UDP/TCP-Port; der Standardwert ist 161.
Login	**login**	Der Login-Name für den Zugriff auf das Gerät.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
SNMP Version	**snmp_version**	Die zu verwendende SNMP-Version (1, 2c, 3); der Standardwert ist 1.
SNMP Community	**community**	Der SNMP-Community-String; der Standardwert ist **private**.
SNMP Security Level	**snmp_sec_level**	Die SNMP-Sicherheitsstufe (noAuthNoPriv, authNoPriv, authPriv).
SNMP Authentication Protocol	**snmp_auth_prot**	Das SNMP-Authentifizierungsprotokoll (MD5, SHA).
SNMP Privacy Protocol	**snmp_priv_prot**	Das SNMP-Verschlüsselungsprotokoll (DES, AES).
SNMP Privacy Protocol Password	**snmp_priv_passwd**	Das Passwort für das SNMP-Verschlüsselungsprotokoll.
SNMP Privacy Protocol Script	**snmp_priv_passwd_script**	Das Skript, das ein Passwort für das SNMP-Verschlüsselungsprotokoll liefert. Dies ersetzt den **SNMP privacy protocol password** Parameter.
Power Wait (seconds)	**power_wait**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	**power_timeout**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	**shell_timeout**	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	**login_timeout**	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	**retry_on**	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Port (Outlet) Number	**port**	Der Port.
Delay (optional)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.

Tabelle A.4, „Brocade Fabric Switch“ listet die Fencing-Geräteparameter, die von **fence_brocade** - dem Fencing-Agenten für Brocade FC Switches - verwendet werden.

Tabelle A.4. Brocade Fabric Switch

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das mit dem Cluster verbundene Brocade-Gerät.
IP Address or Hostname	**ipaddr**	Die IP-Adresse des Geräts.
Login	**login**	Der Login-Name für den Zugriff auf das Gerät.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
Port	**port**	Die Switch-Outlet-Nummer.
Unfencing	**unfence** Abschnitt der Cluster-Konfigurations-datei	Wenn aktiviert, stellt dies sicher, dass ein abgegrenzter Knoten erst wieder reaktiviert wird, nachdem er neu gestartet wurde. Dies ist notwendig für andere Fencing-Methoden als das Power-Fencing (also SAN/Speicher-Fencing). Wenn Sie ein Gerät konfigurieren, dass Unfencing (Aufheben der Knotenabgrenzung) erfordert, muss der Cluster zunächst gestoppt werden, dann muss die vollständige Konfiguration einschließlich Geräte und Unfencing hinzugefügt werden, bevor der Cluster gestartet wird. Informationen über das Unfencing finden Sie auf der **fence_node**(8) Handbuchseite. Für Informationen über das Konfigurieren von Unfencing in der Cluster-Konfigurationsdatei werfen Sie einen Blick auf Abschnitt 7.3, „Konfiguration von Fencing“. Für Informationen über das Konfigurieren von Unfencing mit dem **ccs** Befehl werfen Sie einen Blick auf Abschnitt 5.7.2, „Konfiguration eines einzelnen Speicher-Fencing-Geräts für einen Knoten“.

Tabelle A.5, „Cisco MDS“ listet die Fencing-Geräteparameter, die von **fence_cisco_mds** - dem Fencing-Agenten für Cisco MDS - verwendet werden.

Tabelle A.5. Cisco MDS

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das Cisco MDS 9000 Series Gerät mit aktiviertem SNMP.
IP Address or Hostname	**ipaddr**	Die IP-Adresse oder der Hostname des Geräts.
UDP/TCP port (optional)	**udpport**	Der zur Verbindung mit diesem Gerät zu verwendende UDP/TCP-Port; der Standardwert ist 161.
Login	**login**	Der Login-Name für den Zugriff auf das Gerät.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
SNMP Version	**snmp_version**	Die zu verwendende SNMP-Version (1, 2c, 3).
SNMP Community	**community**	Der SNMP-Community-String.
SNMP Security Level	**snmp_sec_level**	Die SNMP-Sicherheitsstufe (noAuthNoPriv, authNoPriv, authPriv).
SNMP Authentication Protocol	**snmp_auth_prot**	Das SNMP-Authentifizierungsprotokoll (MD5, SHA).
SNMP Privacy Protocol	**snmp_priv_prot**	Das SNMP-Verschlüsselungsprotokoll (DES, AES).
SNMP Privacy Protocol Password	**snmp_priv_passwd**	Das Passwort für das SNMP-Verschlüsselungsprotokoll.
SNMP Privacy Protocol Script	**snmp_priv_passwd_script**	Das Skript, das ein Passwort für das SNMP-Verschlüsselungsprotokoll liefert. Dies ersetzt den **SNMP privacy protocol password** Parameter.
Power Wait (seconds)	**power_wait**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	**power_timeout**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	**shell_timeout**	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	**login_timeout**	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	**retry_on**	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Port (Outlet) Number	**port**	Der Port.
Delay (optional)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.

Tabelle A.6, „Cisco UCS“ listet die Fencing-Geräteparameter, die von **fence_cisco_ucs** - dem Fencing-Agenten für Cisco UCS - verwendet werden.

Tabelle A.6. Cisco UCS

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das Cisco UCS-Gerät.
IP Address or Hostname	**ipaddr**	Die IP-Adresse oder der Hostname des Geräts.
IP port (optional)	**ipport**	Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port.
Login	**login**	Der Login-Name für den Zugriff auf das Gerät.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
Use SSL	**ssl**	SSL-Verbindungen zur Kommunikation mit dem Gerät verwenden.
Sub-Organization	**suborg**	Zusätzlicher Pfad zum Zugriff auf Unterorganisation.
Power Wait (seconds)	**power_wait**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	**power_timeout**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	**shell_timeout**	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	**login_timeout**	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	**retry_on**	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Port (Outlet) Number	**port**	Name der virtuellen Maschine.
Delay (optional)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.

Tabelle A.7, „Dell DRAC 5“ listet die Fencing-Geräteparameter, die von **fence_drac5** - dem Fencing-Agent für Dell DRAC 5 - verwendet werden.

Tabelle A.7. Dell DRAC 5

luci-Feld	cluster.conf Parameter	Beschreibung
Name	`name`	Der dem DRAC zugewiesene Name.
IP Address or Hostname	`ipaddr`	Die IP-Adresse oder der Hostname für den DRAC.
IP-Port (optional)	`ipport`	Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port.
Login	`login`	Der Login-Name für den Zugriff auf den DRAC.
Password	`passwd`	Das Passwort zur Authentifizierung der Verbindung mit dem DRAC.
Password Script (optional)	`passwd_script`	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
Use SSH	`secure`	Zeigt an, dass das System SSH zum Zugriff auf das Gerät verwendet. Bei der Verwendung von SSH müssen Sie entweder ein Passwort, ein Passwortskript oder eine Identitätsdatei angeben.
Path to SSH Identity File	`identity_file`	Die Identitätsdatei für SSH.
Module Name	`module_name`	(optional) Der Modulname für den DRAC, wenn Sie mehrere DRAC-Module haben.
Force Command Prompt	`cmd_prompt`	Die zu verwendende Eingabeaufforderung. Der Standardwert ist ’\$’.
Power Wait (seconds)	`power_wait`	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Delay (seconds)	`delay`	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.
Power Timeout (seconds)	`power_timeout`	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	`shell_timeout`	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	`login_timeout`	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	`retry_on`	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.

Tabelle A.8, „Eaton Netzwerk Stromversorgungs-Schalter Steuerung (SNMP Schnittstelle) (Red Hat Enterprise Linux 6.4 und höher)“ listet die Fencing-Geräteparameter, die von **`fence_eaton_snmp`** - dem Fencing-Agent für den Eaton über SNMP Network Power Switch - verwendet werden.

Tabelle A.8. Eaton Netzwerk Stromversorgungs-Schalter Steuerung (SNMP Schnittstelle) (Red Hat Enterprise Linux 6.4 und höher)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für den mit dem Cluster verbundenen Eaton Netzwerk Stromversorgungs-Schalter.
IP Address or Hostname	**ipaddr**	Die IP-Adresse oder der Hostname des Geräts.
UDP/TCP Port (optional)	**udpport**	Der zur Verbindung mit diesem Gerät zu verwendende UDP/TCP-Port; der Standardwert ist 161.
Login	**login**	Der Login-Name für den Zugriff auf das Gerät.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
SNMP Version	**snmp_version**	Die zu verwendende SNMP-Version (1, 2c, 3); der Standardwert ist 1.
SNMP Community	**community**	Der SNMP-Community-String; der Standardwert ist **private**.
SNMP Security Level	**snmp_sec_level**	Die SNMP-Sicherheitsstufe (noAuthNoPriv, authNoPriv, authPriv).
SNMP Authentication Protocol	**snmp_auth_prot**	Das SNMP-Authentifizierungsprotokoll (MD5, SHA).
SNMP Privacy Protocol	**snmp_priv_prot**	Das SNMP-Verschlüsselungsprotokoll (DES, AES).
SNMP Privacy Protocol Password	**snmp_priv_passwd**	Das Passwort für das SNMP-Verschlüsselungsprotokoll.
SNMP Privacy Protocol Script	**snmp_priv_passwd_script**	Das Skript, das ein Passwort für das SNMP-Verschlüsselungsprotokoll liefert. Dies ersetzt den **SNMP privacy protocol password** Parameter.
Power Wait (seconds)	**power_wait**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	**power_timeout**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	**shell_timeout**	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	**login_timeout**	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	**retry_on**	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Port (Outlet) Number	**port**	Physische Anschlussnummer oder Name der virtuellen Maschine. Dieser Parameter ist immer erforderlich.
Delay (optional)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.

Tabelle A.9, „Egenera SAN-Controller“ listet die Fencing-Geräteparameter, die von **fence_egenera** - dem Fencing-Agent für Egenera BladeFrame - verwendet werden.

Tabelle A.9. Egenera SAN-Controller

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das mit dem Cluster verbundene Egenera BladeFrame-Gerät.
CServer	**cserver**	Der dem Gerät zugewiesene Hostname (und optional der Benutzername in der Form **username@hostname**). Siehe die fence_egenera(8) Handbuchseite für weitere Informationen.
ESH Path (optional)	**esh**	Der Pfad zum esh-Befehl auf dem cserver (Standard ist /opt/panmgr/bin/esh)
Username	**user**	Der Loginname. Der Standardwert ist **root**.
lpan	**lpan**	Das Logical Process Area Network (LPAN) des Geräts.
pserver	**pserver**	Der Name des Processing Blade (pserver) des Geräts.
Delay (optional)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.
Unfencing	**unfence** Abschnitt der Cluster-Konfigurations-datei	Wenn aktiviert, stellt dies sicher, dass ein abgegrenzter Knoten erst wieder reaktiviert wird, nachdem er neu gestartet wurde. Dies ist notwendig für andere Fencing-Methoden als das Power-Fencing (also SAN/Speicher-Fencing). Wenn Sie ein Gerät konfigurieren, dass Unfencing (Aufheben der Knotenabgrenzung) erfordert, muss der Cluster zunächst gestoppt werden, dann muss die vollständige Konfiguration einschließlich Geräte und Unfencing hinzugefügt werden, bevor der Cluster gestartet wird. Informationen über das Unfencing finden Sie auf der **fence_node**(8) Handbuchseite. Für Informationen über das Konfigurieren von Unfencing in der Cluster-Konfigurationsdatei werfen Sie einen Blick auf Abschnitt 7.3, „Konfiguration von Fencing“. Für Informationen über das Konfigurieren von Unfencing mit dem **ccs** Befehl werfen Sie einen Blick auf Abschnitt 5.7.2, „Konfiguration eines einzelnen Speicher-Fencing-Geräts für einen Knoten“.

Tabelle A.10, „ePowerSwitch“ listet die Fencing-Geräteparameter, die von **fence_eps** - dem Fencing-Agent für ePowerSwitch - verwendet werden.

Tabelle A.10. ePowerSwitch

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das mit dem Cluster verbundene ePowerSwitch-Gerät.
IP Address or Hostname	**ipaddr**	Die IP-Adresse oder der Hostname des Geräts.
Login	**login**	Der Login-Name für den Zugriff auf das Gerät.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
Name of Hidden Page	**hidden_page**	Der Name der Hidden Page für das Gerät.
Times to Retry Power On Operation	**retry_on**	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Port (Outlet) Number	**port**	Physische Anschlussnummer oder Name der virtuellen Maschine.
Delay (optional)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.

Tabelle A.11, „Fence virt“ listet die Fencing-Geräteparameter, die von **fence_virt** - dem Fencing-Agenten für ein Fence-virt-fence-Gerät - verwendet werden.

Tabelle A.11. Fence virt

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das Fence virt Fencing-Gerät.
Serial Device	**serial_device**	Auf dem Host muss das serielle Gerät in der Konfigurationsdatei einer jeden Domain zugewiesen sein. Für weitere Informationen siehe die **fence_virt.conf** Handbuchseite. Ist dieses Feld angegeben, veranlasst dies den **fence_virt** Fencing-Agenten zum Betrieb im seriellen Modus. Wird kein Wert angegeben, veranlasst dies den **fence_virt** Fencing-Agenten zum Betrieb im VM-Channel-Modus.
Serial Parameters	**serial_params**	Die seriellen Parameter. Der Standard ist 115200, 8N1.
VM Channel IP Adresse	**channel_address**	Die Channel-IP. Der Standardwert ist 10.0.2.179.
Port or Domain (deprecated)	**port**	Die abzugrenzende virtuelle Maschine (Domain-UUID oder Name).
	ipport	Der Channel-Port. Der Standardwert ist 1229, dieser Wert wird verwendet, wenn das Fencing-Gerät mit **luci** konfiguriert wird.

Tabelle A.12, „Fujitsu Siemens Remoteview Service Board (RSB)“ listet die Fencing-Geräteparameter, die von **fence_rsb** - dem Fencing-Agent für Fujitsu-Siemens RSB - verwendet werden.

Tabelle A.12. Fujitsu Siemens Remoteview Service Board (RSB)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	`name`	Ein Name des RSB, das als Fencing-Gerät verwendet werden soll.
IP Address or Hostname	`ipaddr`	Der Hostname des Geräts.
Login	`login`	Der Login-Name für den Zugriff auf das Gerät.
Password	`passwd`	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	`passwd_script`	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
TCP Port	`ipport`	Die Port-Nummer, auf dem der telnet-Dienst horcht. Der Standardwert ist 3172.
Force Command Prompt	`cmd_prompt`	Die zu verwendende Eingabeaufforderung. Der Standardwert ist '\$'.
Power Wait (seconds)	`power_wait`	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Delay (seconds)	`delay`	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.
Power Timeout (seconds)	`power_timeout`	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	`shell_timeout`	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	`login_timeout`	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	`retry_on`	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.

Tabelle A.13, „HP BladeSystem (Red Hat Enterprise Linux 6.4 und höher)“ listet die Fencing-Geräteparameter, die von **fence_hpblade** - dem Fencing-Agent für das HP Bladesystem - verwendet werden.

Tabelle A.13. HP BladeSystem (Red Hat Enterprise Linux 6.4 und höher)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	name	Der Name für das mit dem Cluster verbundene HP BladeSystem-Gerät.
IP Address or Hostname	ipaddr	Die IP-Adresse oder der Hostname, der dem HP BladeSystem zugeordnet ist.
IP-Port (optional)	ipport	Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port.
Login	login	Der Login-Name für den Zugriff auf das HP BladeSystem Gerät. Dieser Parameter ist notwendig.
Password	passwd	Das Passwort zur Authentifizierung der Verbindung mit dem Fencing-Gerät.
Password Script (optional)	passwd_script	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
Force Command Prompt	cmd_prompt	Die zu verwendende Eingabeaufforderung. Der Standardwert ist '\$'.
Missing port returns OFF instead of failure	missing_as_off	Fehlender Port gibt OFF statt Misserfolg zurück.
Power Wait (seconds)	power_wait	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	power_timeout	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	shell_timeout	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	login_timeout	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	retry_on	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Use SSH	secure	Zeigt an, dass das System SSH zum Zugriff auf das Gerät verwendet. Bei der Verwendung von SSH müssen Sie entweder ein Passwort, ein Passwortskript oder eine Identitätsdatei angeben.
Path to SSH Identity File	identity_file	Die Identitätsdatei für SSH.

Die Fencing-Agents für HP iLO Geräte **fence_ilo** und HP iLO2 Geräte **fence_ilo2** verwenden dieselbe Implementation. Tabelle A.14, „HP iLO (Integrated Lights Out) und HP iLO2“ listet die Fencing-Geräteparameter auf, die von diesen Agents verwendet werden.

Tabelle A.14. HP iLO (Integrated Lights Out) und HP iLO2

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für den Server mit HP iLO Unterstützung.
IP Address or Hostname	**ipaddr**	Die IP-Adresse oder der Hostname des Geräts.
IP-Port (optional)	**ipport**	Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port.
Login	**login**	Der Login-Name für den Zugriff auf das Gerät.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
Power Wait (seconds)	**power_wait**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Delay (seconds)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.
Power Timeout (seconds)	**power_timeout**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	**shell_timeout**	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	**login_timeout**	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	**retry_on**	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.

Tabelle A.15, „HP iLO (Integrated Lights Out) MP“ listet die Fencing-Geräteparameter, die von **fence_ilo_mp** - dem Fencing-Agenten für HP-iLO-MP-Geräte - verwendet werden.

Tabelle A.15. HP iLO (Integrated Lights Out) MP

luci-Feld	cluster.conf Parameter	Beschreibung
Name	`name`	Ein Name für den Server mit HP iLO Unterstützung.
IP Address or Hostname	`ipaddr`	Die IP-Adresse oder der Hostname des Geräts.
IP-Port (optional)	`ipport`	Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port.
Login	`login`	Der Login-Name für den Zugriff auf das Gerät.
Password	`passwd`	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	`passwd_script`	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
Use SSH	`secure`	Zeigt an, dass das System SSH zum Zugriff auf das Gerät verwendet. Bei der Verwendung von SSH müssen Sie entweder ein Passwort, ein Passwortskript oder eine Identitätsdatei angeben.
Path to SSH Identity File	`identity_file`	Die Identitätsdatei für SSH.
Force Command Prompt	`cmd_prompt`	Die zu verwendende Eingabeaufforderung. Der Standardwert ist 'MP>', 'hpiLO->'.
Power Wait (seconds)	`power_wait`	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Delay (seconds)	`delay`	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.
Power Timeout (seconds)	`power_timeout`	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	`shell_timeout`	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	`login_timeout`	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	`retry_on`	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.

Tabelle A.16, „IBM BladeCenter“ listet die Fencing-Geräteparameter, die von **`fence_bladecenter`** - dem Fencing-Agent für IBM BladeCenter - verwendet werden.

Tabelle A.16. IBM BladeCenter

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das mit dem Cluster verbundene IBM BladeCenter-Gerät.
IP Address or Hostname	**ipaddr**	Die IP-Adresse oder der Hostname des Geräts.
IP port (optional)	**ipport**	Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port.
Login	**login**	Der Login-Name für den Zugriff auf das Gerät.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
Power Wait (seconds)	**power_wait**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	**power_timeout**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	**shell_timeout**	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	**login_timeout**	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	**retry_on**	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Use SSH	**secure**	Zeigt an, dass das System SSH zum Zugriff auf das Gerät verwendet. Bei der Verwendung von SSH müssen Sie entweder ein Passwort, ein Passwortskript oder eine Identitätsdatei angeben.
Path to SSH Identity File	**identity_file**	Die Identitätsdatei für SSH.

Tabelle A.17, „IBM BladeCenter SNMP“ listet die Fencing-Geräteparameter, die von **fence_ibmblade** - dem Fencing-Agenten für IBM BladeCenter über SNMP - verwendet werden.

Tabelle A.17. IBM BladeCenter SNMP

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das mit dem Cluster verbundene IBM BladeCenter SNMP-Gerät.
IP Address or Hostname	**ipaddr**	Die IP-Adresse oder der Hostname des Geräts.
UDP/TCP Port (optional)	**udpport**	Der zur Verbindung mit diesem Gerät zu verwendende UDP/TCP-Port; der Standardwert ist 161.
Login	**login**	Der Login-Name für den Zugriff auf das Gerät.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
SNMP Version	**snmp_version**	Die zu verwendende SNMP-Version (1, 2c, 3); der Standardwert ist 1.
SNMP Community	**community**	Der SNMP-Community-String.
SNMP Security Level	**snmp_sec_level**	Die SNMP-Sicherheitsstufe (noAuthNoPriv, authNoPriv, authPriv).
SNMP Authentication Protocol	**snmp_auth_prot**	Das SNMP-Authentifizierungsprotokoll (MD5, SHA).
SNMP Privacy Protocol	**snmp_priv_prot**	Das SNMP-Verschlüsselungsprotokoll (DES, AES).
SNMP privacy protocol password	**snmp_priv_passwd**	Das Passwort für das SNMP-Verschlüsselungsprotokoll.
SNMP Privacy Protocol Script	**snmp_priv_passwd_script**	Das Skript, das ein Passwort für das SNMP-Verschlüsselungsprotokoll liefert. Dies ersetzt den **SNMP privacy protocol password** Parameter.
Power Wait (seconds)	**power_wait**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	**power_timeout**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	**shell_timeout**	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	**login_timeout**	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	**retry_on**	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Port (Outlet) Number	**port**	Physische Anschlussnummer oder Name der virtuellen Maschine.
Delay (optional)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.

Tabelle A.18, „IBM iPDU (Red Hat Enterprise Linux 6.4 und höher)“ listet die Fencing-Geräteparameter, die von **fence_ipdu** - dem Fencing-Agenten für iPDU over SNMP-Geräten - verwendet werden.

Tabelle A.18. IBM iPDU (Red Hat Enterprise Linux 6.4 und höher)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das mit dem Cluster verbundene IBM iPDU Gerät, bei dem sich der Fencing-Daemon über das SNMP-Protokoll anmeldet.
IP Address or Hostname	**ipaddr**	Die IP-Adresse oder der Hostname des Geräts.
UDP/TCP Port	**udpport**	Der zur Verbindung mit diesem Gerät zu verwendende UDP/TCP-Port; der Standardwert ist 161.
Login	**login**	Der Login-Name für den Zugriff auf das Gerät.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
SNMP Version	**snmp_version**	Die zu verwendende SNMP-Version (1, 2c, 3); der Standardwert ist 1.
SNMP Community	**community**	Der SNMP-Community-String; der Standardwert ist **private**.
SNMP Security Level	**snmp_sec_level**	Die SNMP-Sicherheitsstufe (noAuthNoPriv, authNoPriv, authPriv).
SNMP Authentication Protocol	**snmp_auth_prot**	Das SNMP-Authentifizierungsprotokoll (MD5, SHA).
SNMP Privacy Protocol	**snmp_priv_prot**	Das SNMP-Verschlüsselungsprotokoll (DES, AES).
SNMP Privacy Protocol Password	**snmp_priv_passwd**	Das Passwort für das SNMP-Verschlüsselungsprotokoll.
SNMP Privacy Protocol Script	**snmp_priv_passwd_script**	Das Skript, das ein Passwort für das SNMP-Verschlüsselungsprotokoll liefert. Dies ersetzt den **SNMP privacy protocol password** Parameter.
Power Wait (seconds)	**power_wait**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	**power_timeout**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	**shell_timeout**	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	**login_timeout**	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	**retry_on**	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Port (Outlet) Number	**port**	Physische Anschlussnummer oder Name der virtuellen Maschine.
Delay (optional)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.

Tabelle A.19, „IF MIB“ listet die Fencing-Geräteparameter, die von **fence_ifmib** - dem Fencing-Agenten für IF-MIB-Geräte - verwendet werden.

Tabelle A.19. IF MIB

luci-Feld	cluster.conf Parameter	Beschreibung
Name	`name`	Ein Name für das mit dem Cluster verbundene IF MIB-Gerät.
IP Address or Hostname	`ipaddr`	Die IP-Adresse oder der Hostname des Geräts.
UDP/TCP Port (optional)	`udpport`	Der zur Verbindung mit diesem Gerät zu verwendende UDP/TCP-Port; der Standardwert ist 161.
Login	`login`	Der Login-Name für den Zugriff auf das Gerät.
Password	`passwd`	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	`passwd_script`	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
SNMP Version	`snmp_version`	Die zu verwendende SNMP-Version (1, 2c, 3); der Standardwert ist 1.
SNMP Community	`community`	Der SNMP-Community-String.
SNMP Security Level	`snmp_sec_level`	Die SNMP-Sicherheitsstufe (noAuthNoPriv, authNoPriv, authPriv).
SNMP Authentication Protocol	`snmp_auth_prot`	Das SNMP-Authentifizierungsprotokoll (MD5, SHA).
SNMP Privacy Protocol	`snmp_priv_prot`	Das SNMP-Verschlüsselungsprotokoll (DES, AES).
SNMP Privacy Protocol Password	`snmp_priv_passwd`	Das Passwort für das SNMP-Verschlüsselungsprotokoll.
SNMP Privacy Protocol Script	`snmp_priv_passwd_script`	Das Skript, das ein Passwort für das SNMP-Verschlüsselungsprotokoll liefert. Dies ersetzt den **SNMP privacy protocol password** Parameter.
Power Wait (seconds)	`power_wait`	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	`power_timeout`	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	`shell_timeout`	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	`login_timeout`	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	`retry_on`	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Port (Outlet) Number	`port`	Physische Anschlussnummer oder Name der virtuellen Maschine.
Delay (optional)	`delay`	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.

Tabelle A.20, „Intel Modular“ listet die Fencing-Geräteparameter, die von **`fence_intelmodular`** - dem Fencing-Agenten für Intel Modular - verwendet werden.

Tabelle A.20. Intel Modular

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das mit dem Cluster verbundene Intel Modular-Gerät.
IP Address or Hostname	**ipaddr**	Die IP-Adresse oder der Hostname des Geräts.
UDP/TCP Port (optional)	**udpport**	Der zur Verbindung mit diesem Gerät zu verwendende UDP/TCP-Port; der Standardwert ist 161.
Login	**login**	Der Login-Name für den Zugriff auf das Gerät.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
SNMP Version	**snmp_version**	Die zu verwendende SNMP-Version (1, 2c, 3); der Standardwert ist 1.
SNMP Community	**community**	Der SNMP-Community-String; der Standardwert ist **private**.
SNMP Security Level	**snmp_sec_level**	Die SNMP-Sicherheitsstufe (noAuthNoPriv, authNoPriv, authPriv).
SNMP Authentication Protocol	**snmp_auth_prot**	Das SNMP-Authentifizierungsprotokoll (MD5, SHA).
SNMP Privacy Protocol	**snmp_priv_prot**	Das SNMP-Verschlüsselungsprotokoll (DES, AES).
SNMP Privacy Protocol Password	**snmp_priv_passwd**	Das Passwort für das SNMP-Verschlüsselungsprotokoll.
SNMP Privacy Protocol Script	**snmp_priv_passwd_script**	Das Skript, das ein Passwort für das SNMP-Verschlüsselungsprotokoll liefert. Dies ersetzt den **SNMP privacy protocol password** Parameter.
Power Wait (seconds)	**power_wait**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	**power_timeout**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	**shell_timeout**	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	**login_timeout**	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	**retry_on**	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Port (Outlet) Number	**port**	Physische Anschlussnummer oder Name der virtuellen Maschine.
Delay (optional)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.

Die Fencing-Agents für IPMI über LAN (**fence_ipmilan**,) Dell iDRAC (**fence_idrac**), IBM Integriertes Managementmodul (**fence_imm**), HP iLO3 Geräte **fence_ilo3** und HP iLO4 Geräte **fence_ilo4** verwenden dieselbe Implementation. Tabelle A.21, „IPMI (Intelligent Platform Management Interface) LAN, Dell iDrac, IBM Integriertes Managementmodul, HPiLO3, HPiLO4“ listet die Fencing-

Geräteparameter auf, die von diesen Agents verwendet werden.

Tabelle A.21. IPMI (Intelligent Platform Management Interface) LAN, Dell iDrac, IBM Integriertes Managementmodul, HPiLO3, HPiLO4

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das Fencing-Gerät, das mit dem Cluster verbunden ist.
IP Address or Hostname	**ipaddr**	Die IP-Adresse oder der Hostname des Geräts.
Login	**login**	Der Login-Name eines Benutzers, der Befehle zum Ein- und Ausschalten des angegebenen Ports ausgeben darf.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Port.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
Authentication Type	**auth**	Authentifizierungstyp: **none**, **password** oder **MD5**.
Use Lanplus	**lanplus**	**True** oder **1**. Falls leer, ist der Wert **False**. Es wird empfohlen, dass Sie Lanplus aktivieren, um die Sicherheit Ihrer Verbindung zu erhöhen, sofern Ihre Hardware dies unterstützt.
Ciphersuite to use	**cipher**	Die Remote-Server-Authentifizierung, Integrität und Verschlüsselungs-Algorithmen, die für IPMIv2 lanplus Verbindungen verwendet werden.
Privilege level	**privlvl**	Das Berechtigungslevel auf dem Gerät.
IPMI Operation Timeout	**timeout**	Timeout in Sekunden für IPMI-Operation.
Power Wait (seconds)	**power_wait**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Delay (optional)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.

Tabelle A.22, „RHEV-M REST API (RHEL 6.2 und höher mit RHEV 3.0 und höher)“ listet die Fencing-Geräteparameter, die von **fence_rhevm** - dem Fencing-Agenten für RHEV-M REST API - verwendet werden.

Tabelle A.22. RHEV-M REST API (RHEL 6.2 und höher mit RHEV 3.0 und höher)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	`name`	Der Name des RHEV-M REST API Fencing-Geräts.
IP Address or Hostname	`ipaddr`	Die IP-Adresse oder der Hostname des Geräts.
IP-Port (optional)	`ipport`	Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port.
Login	`login`	Der Login-Name für den Zugriff auf das Gerät.
Password	`passwd`	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	`passwd_script`	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
Use SSL	`ssl`	SSL-Verbindungen zur Kommunikation mit dem Gerät verwenden.
Power Wait (seconds)	`power_wait`	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	`power_timeout`	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	`shell_timeout`	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	`login_timeout`	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	`retry_on`	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Port (Outlet) Number	`port`	Physische Anschlussnummer oder Name der virtuellen Maschine.
Delay (optional)	`delay`	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.

Tabelle A.23, „SCSI Reservation Fencing“ listet die Fencing-Geräteparameter, die von **`fence_scsi`** - dem Fencing-Agenten für SCSI persistente Reservierungen - verwendet werden.



Anmerkung

Die Verwendung von SCSI persistenten Reservierungen als Fencing-Methode wird zwar unterstützt, unterliegt jedoch den folgenden Einschränkungen:

- Bei der Verwendung von SCSI-Fencing müssen sich alle Knoten im Cluster bei demselben Gerät registrieren, damit jeder Knoten den Registrierungsschlüssel eines anderen Knotens von allen Geräten entfernen kann, bei denen er registriert ist.
- Bei den Geräten, die als Cluster-Datenträger eingesetzt werden, sollte es sich um komplette LUNs handeln, nicht um Partitionen. SCSI persistente Reservierungen arbeiten auf einer gesamten LUN, was bedeutet, dass der Zugriff auf jede einzelne LUN kontrolliert wird, nicht auf einzelne Partitionen.

Tabelle A.23. SCSI Reservation Fencing

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das SCSI-Fencing-Gerät.
Unfencing	**unfence** Abschnitt der Cluster-Konfigurationsdatei	Wenn aktiviert, stellt dies sicher, dass ein abgegrenzter Knoten erst wieder reaktiviert wird, nachdem er neu gestartet wurde. Dies ist notwendig für andere Fencing-Methoden als das Power-Fencing (also SAN/Speicher-Fencing). Wenn Sie ein Gerät konfigurieren, dass Unfencing (Aufheben der Knotenabgrenzung) erfordert, muss der Cluster zunächst gestoppt werden, dann muss die vollständige Konfiguration einschließlich Geräte und Unfencing hinzugefügt werden, bevor der Cluster gestartet wird. Informationen über das Unfencing finden Sie auf der **fence_node**(8) Handbuchseite. Für Informationen über das Konfigurieren von Unfencing in der Cluster-Konfigurationsdatei werfen Sie einen Blick auf Abschnitt 7.3, „Konfiguration von Fencing“. Für Informationen über das Konfigurieren von Unfencing mit dem **ccs** Befehl werfen Sie einen Blick auf Abschnitt 5.7.2, „Konfiguration eines einzelnen Speicher-Fencing-Geräts für einen Knoten“.
Node name	**nodename**	Der Knotenname wird verwendet, um den Schlüsselwert für die aktuelle Operation zu generieren.
Key for current action	**key**	(setzt Knotenname außer Kraft) Schlüssel für die aktuelle Operation. Dieser Schlüssel sollte eindeutig auf dem Knoten sein. Für die "on"-Aktion spezifiziert der Schlüssel den zur Registrierung des lokalen Knoten zu verwendenden Schlüssel. Für die "off"-Aktion spezifiziert dieser Schlüssel den von den Geräten zu entfernenden Schlüssel.
Delay (optional)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.

Tabelle A.24, „VMware Fencing (SOAP-Schnittstelle) (Red Hat Enterprise Linux 6.2 und höher)“ listet die Fencing-Geräteparameter, die von **fence_vmware_soap** - dem Fencing-Agenten für VMWare über SOAP-API - verwendet werden.

Tabelle A.24. VMware Fencing (SOAP-Schnittstelle) (Red Hat Enterprise Linux 6.2 und höher)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein Name für das Fence virt Fencing-Gerät.
IP Address or Hostname	**ipaddr**	Die IP-Adresse oder der Hostname des Geräts.
IP-Port (optional)	**ipport**	Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port.
Login	**login**	Der Login-Name für den Zugriff auf das Gerät.
Password	**passwd**	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	**passwd_script**	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
Power Wait (seconds)	**power_wait**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	**power_timeout**	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	**shell_timeout**	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	**login_timeout**	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	**retry_on**	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
VM name	**port**	Name der virtuellen Maschine im Inventarpfad-Format (z.B. /datacenter/vm/Discovered_virtual_machine/myMachine).
VM UUID	**uuid**	Die UUID der abzugrenzenden virtuellen Maschine.
Delay (optional)	**delay**	Anzahl von Sekunden, die gewartet werden soll, bevor die Abgrenzung gestartet wird. Der Standardwert ist 0.
Use SSL	**ssl**	SSL-Verbindungen zur Kommunikation mit dem Gerät verwenden.

Tabelle A.25, „WTI Power Switch“ listet die Fencing-Geräteparameter, die von **fence_wti** - dem Fencing-Agenten für den WTI Network Power Switch - verwendet werden.

Tabelle A.25. WTI Power Switch

luci-Feld	cluster.conf Parameter	Beschreibung
Name	`name`	Ein Name für den mit dem Cluster verbundenen WTI Power Switch.
IP Address or Hostname	`ipaddr`	Die IP-Adresse oder der Hostname des Geräts.
IP-Port (optional)	`ipport`	Der zur Verbindung mit diesem Gerät zu verwendende TCP-Port.
Login	`login`	Der Login-Name für den Zugriff auf das Gerät.
Password	`passwd`	Das Passwort zur Authentifizierung der Verbindung mit dem Gerät.
Password Script (optional)	`passwd_script`	Das Skript, das ein Passwort zum Zugriff auf das Fencing-Gerät liefert. Dies ersetzt den **Password** Parameter.
Force command prompt	`cmd_prompt`	Die zu verwendende Eingabeaufforderung. Der Standardwert ist [’RSM>’, ’>MPC’, ’IPS>’, ’TPS>’, ’NBB>’, ’NPS>’, ’VMR>’]
Power Wait (seconds)	`power_wait`	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll.
Power Timeout (seconds)	`power_timeout`	Anzahl von Sekunden, die nach einem Befehl zum Ein- oder Ausschalten gewartet werden soll, bevor auf eine Statusänderung hin überprüft wird. Der Standardwert ist 20.
Shell Timeout (seconds)	`shell_timeout`	Anzahl von Sekunden, die nach Eingabe eines Befehl auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 3.
Login Timeout (seconds)	`login_timeout`	Anzahl von Sekunden, die nach der Anmeldung auf die Eingabeaufforderung gewartet werden soll. Der Standardwert ist 5.
Times to Retry Power On Operation	`retry_on`	Anzahl von Neuversuchen für einen Befehl zum Anschalten. Der Standardwert ist 1.
Use SSH	`secure`	Zeigt an, dass das System SSH zum Zugriff auf das Gerät verwendet. Bei der Verwendung von SSH müssen Sie entweder ein Passwort, ein Passwortskript oder eine Identitätsdatei angeben.
Path to SSH Identity File	`identity_file`	Die Identitätsdatei für SSH.
Port	`port`	Physische Anschlussnummer oder Name der virtuellen Maschine.

Parameter der Hochverfügbarkeitsressourcen

Dieser Anhang beschreibt die Parameter der Hochverfügbarkeitsressource. Sie können diese Parameter mithilfe von **luci** oder unter Verwendung des **ccs** Befehls konfigurieren, oder indem Sie die **etc/cluster/cluster.conf** Datei bearbeiten. Tabelle B.1, „Übersicht über Hochverfügbarkeitsressourcen“ listet die Ressourcen, ihre zugehörigen Ressourcen-Agenten, sowie Verweise auf andere Tabellen mit Parameterbeschreibungen. Für ein besseres Verständnis von Ressourcen-Agenten können Sie sich diese in **/usr/share/cluster** in jedem beliebigen Cluster-Knoten ansehen.

Neben den in diesem Anhang beschriebenen Ressourcen-Agenten enthält das **/usr/share/cluster** Verzeichnis auch eine OCF-Skriptvorlage für eine Ressourcen-Gruppe **service.sh**. Weitere Informationen über die in diesem Skript enthaltenen Parameter finden Sie im **service.sh** Skript selbst.

Eine vollständigere Liste samt Beschreibung aller **cluster.conf** Elemente und Parameter finden Sie im Cluster-Schema unter **/usr/share/cluster/cluster.rng** und im kommentierten Schema unter **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (zum Beispiel **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

Tabelle B.1. Übersicht über Hochverfügbarkeitsressourcen

Ressource	Ressourcen-Agent	Verweis auf Parameterbeschreibung
Apache	apache.sh	Tabelle B.2, „Apache (**apache**-Ressource)“
Condor-Instanz	condor.sh	Tabelle B.3, „Condor-Instanz (**condor**-Ressource)“
Dateisystem	fs.sh	Tabelle B.4, „Dateisystem (**fs**-Ressource)“
GFS2	clusterfs.sh	Tabelle B.5, „GFS2 (**clusterfs**-Ressource)“
IP-Adresse	ip.sh	Tabelle B.6, „IP-Adresse (**ip**-Ressource)“
HA-LVM	lvm.sh	Tabelle B.7, „HA LVM (**lvm**-Ressource)“
MySQL	mysql.sh	Tabelle B.8, „MySQL (**mysql**-Ressource)“
NFS/CIFS Mount	netfs.sh	Tabelle B.9, „NFS/CIFS Mount (**netfs**-Ressource)“
NFS Client	nfsclient.sh	Tabelle B.10, „NFS Client (**nfsclient**-Ressource)“
NFS v3 Export	nfsexport.sh	Tabelle B.11, „NFS v3 Export (**nfsexport**-Ressource)“
NFS Server	nfsserver.sh	Tabelle B.12, „NFS Server (**nfsserver**-Ressource)“
Oracle 10g/11g Ausfallsicherungsinstanz	oracledb.sh	Tabelle B.14, „Oracle 10g/11g Ausfallsicherunsginstanz (**oracledb**-Ressource)“
Oracle 10g/11g Instanz	orainstance.sh	Tabelle B.15, „Oracle 10g/11g Ausfallsicherungsinstanz (**orainstance**-Ressource)“
Oracle 10g/11g Listener	oralistener.sh	Tabelle B.16, „Oracle 10g/11g Listener (**oralistener**-Ressource)“
Open LDAP	openldap.sh	Tabelle B.13, „Open LDAP (**openldap**-Ressource)“
PostgreSQL 8	postgres-8.sh	Tabelle B.17, „PostgreSQL 8 (**postgrest-8**-Ressource)“
SAP-Datenbank	SAPDatabase	Tabelle B.18, „SAP-Datenbank (**SAPDatabase**-Ressource)“
SAP-Instanz	SAPInstance	Tabelle B.19, „SAP-Instanz (**SAPInstance**-Ressource)“
Samba-Server	samba.sh	Tabelle B.20, „Samba-Server (**samba**-Ressource)“
Skript	script.sh	Tabelle B.21, „Skript (**script**-Ressource)“
Sybase ASE Ausfallsicherungsinstanz	ASEHAagent.sh	Tabelle B.22, „Sybase ASE Ausfallsicherungsinstanz (**ASEHAagent**-Ressource)“
Tomcat 6	tomcat-6.sh	Tabelle B.23, „Tomcat 6 (**tomcat-6**-Ressource)“
Virtuelle Maschine	vm.sh	Tabelle B.24, „Virtuelle Maschine (**vm**-Ressource)“ ANMERKUNG: **Luci** zeigt dies als virtuellen Dienst an, falls der Host-Cluster virtuelle Maschinen unterstützt.

Tabelle B.2. Apache (apache-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Der Name des Apache-Dienstes.
Server Root	**server_root**	Der Standardwert ist **/etc/httpd**.
Config File	**config_file**	Spezifiziert die Apache-Konfigurationsdatei. Der Standardwert ist **/etc/httpd/conf**.
httpd Options	**httpd_options**	Weitere Befehlszeilenoptionen für **httpd**.
Shutdown Wait (seconds)	**shutdown_wait**	Spezifiziert die Anzahl von Sekunden, die auf das korrekte Beenden eines Dienstes gewartet wird.

Tabelle B.3. Condor-Instanz (condor-Ressource)

Feld	luci-Feld	cluster.conf Parameter
Instance Name	**name**	Spezifiziert einen eindeutigen Namen für die Condor-Instanz.
Condor Subsystem Type	**type**	Spezifiziert den Typ des Condor-Subsystems für diese Instanz: **schedd**, **job_server** oder **query_server**.

Tabelle B.4. Dateisystem (fs-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Spezifiziert einen Namen für die Dateisystemressource.
Filesystem Type	**fstype**	Falls nicht angegeben, versucht **mount**, den Dateisystemtyp zu bestimmen.
Mount Point	**mountpoint**	Pfad in der Dateisystemhierarchie, unter dem dieses Dateisystem eingehängt wird.
Device, FS Label, or UUID	**device**	Spezifiziert das Gerät, das mit der Dateisystemressource verknüpft ist. Dabei kann es sich um ein Blockgerät, eine Dateisystemkennung, oder eine UUID eines Dateisystems handeln.
Mount Options	**options**	Einhängeoptionen; also Optionen, die beim Einhängen des Dateisystems angewendet werden. Diese können dateisystemspezifisch sein. Siehe ***mount***(8) Handbuchseite für die unterstützten Einhängeoptionen.
File System ID (optional)	**fsid**	**Anmerkung** ***File System ID*** wird nur von NFS-Diensten verwendet. Beim Erstellen einer neuen Dateisystemressource können Sie dieses Feld leer lassen. Wenn Sie dieses Feld leer lassen, wird automatisch eine Dateisystem-ID zugewiesen, nachdem Sie den Parameter während der Konfiguration übergeben. Wenn Sie explizit eine Dateisystem-ID zuweisen müssen, geben Sie den gewünschten Wert in diesem Feld an.
Force Unmount	**force_unmount**	Falls aktiviert, wird das Dateisystem zum Aushängen gezwungen. Die Standardeinstellung ist ***disabled***. ***Force Unmount*** vernichtet dabei sämtliche Prozesse, die den Einhängepunkt verwenden, damit das eingehängte Dateisystem beim Aushängen nicht mehr verwendet wird.
Force fsck	**force_fsck**	Falls aktiviert, wird **fsck** auf dem Dateisystem ausgeführt, bevor es eingehängt wird. Die Standardeinstellung ist ***disabled***.
Enable NFS daemon and lockd workaround (Red Hat Enterprise Linux 6.4 oder höher)	**nfsrestart**	Wenn Ihr Dateisystem über NFS exportiert wird und manchmal nicht ausgehängt werden kann (entweder beim Herunterfahren oder bei Verlegung des Dienstes), werden durch diese Option alle Dateisystemreferenzen vor dem Aushängen verworfen. Der Einsatz dieser Option erfordert, dass Sie die **Force unmount** Option aktivieren und darf nicht zusammen mit der **NFS Server** Ressource verwendet werden. Sie sollten diese Option nur als letztes Mittel einsetzen, denn dies ist ein vehementer Versuch, ein Dateisystem aushängen.
Use Quick Status Checks	**quick_status**	Falls aktiviert, werden schnelle Statusprüfungen durchgeführt.
Reboot Host Node if Unmount Fails	**self_fence**	Wenn aktiviert, startet den Knoten neu, wenn das Aushängen dieses Dateisystems misslingt. Der **filesystem** Ressourcen-Agent akzeptiert die Werte 1, **yes**, **on** oder **true**, um diesen Parameter zu aktivieren, und die Werte 0, **no**, **off** oder **false**, um ihn zu deaktivieren. Der Standard ist ***disabled***.

Tabelle B.5. GFS2 (`clusterfs`-Ressource)

luci-Feld	`cluster.conf` Parameter	Beschreibung
Name	**`name`**	Der Name der Dateisystemressource.
Mount Point	**`mountpoint`**	Der Pfad, unter dem diese Dateisystemressource eingehängt wird.
Device, FS Label, or UUID	**`device`**	Die Gerätedatei, die mit der Dateisystemressource verknüpft ist.
Filesystem Type	**`fstype`**	Setzen Sie dies auf GFS2 in **luci**
Mount Options	**`options`**	Einhängeoptionen.
File System ID (optional)	**`fsid`**	**Anmerkung** ***`File System ID`*** wird nur von NFS-Diensten verwendet. Beim Erstellen einer neuen GFS2-Ressource können Sie dieses Feld leer lassen. Wenn Sie dieses Feld leer lassen, wird automatisch eine Dateisystem-ID zugewiesen, nachdem Sie den Parameter während der Konfiguration übergeben. Wenn Sie explizit eine Dateisystem-ID zuweisen müssen, geben Sie den gewünschten Wert in diesem Feld an.
Force Unmount	**`force_unmount`**	Falls aktiviert, wird das Dateisystem zum Aushängen gezwungen. Die Standardeinstellung ist ***disabled***. ***`Force Unmount`*** vernichtet dabei sämtliche Prozesse, die den Einhängepunkt verwenden, damit das eingehängte Dateisystem beim Aushängen nicht mehr verwendet wird. Bei GFS2-Ressourcen wird der Einhängepunkt beim Beenden eines Dienstes *nicht* ausgehängt, es sei denn, der ***`Force Unmount`*** ist *enabled*.
Enable NFS daemon and lockd workaround (Red Hat Enterprise Linux 6.4 oder höher)	**`nfsrestart`**	Wenn Ihr Dateisystem über NFS exportiert wird und manchmal nicht ausgehängt werden kann (entweder beim Herunterfahren oder bei Verlegung des Dienstes), werden durch diese Option alle Dateisystemreferenzen vor dem Aushängen verworfen. Der Einsatz dieser Option erfordert, dass Sie die **`Force unmount`** Option aktivieren und darf nicht zusammen mit der **`NFS Server`** Ressource verwendet werden. Sie sollten diese Option nur als letztes Mittel einsetzen, denn dies ist ein vehementer Versuch, ein Dateisystem aushängen.
Reboot Host Node if Unmount Fails	**`self_fence`**	Wenn diese Option aktiviert ist und das Aushängen des Dateisystems fehlschlägt, wird der Knoten sofort neu starten. Im Allgemeinen wird dies in Verbindung mit Force-Unmount Unterstützung verwendet, aber es ist nicht erforderlich. Der **`GFS2`** Ressourcen-Agent akzeptiert die Werte 1, **`yes`**, **`on`** oder **`true`**, um diesen Parameter zu aktivieren, und die Werte 0, **`no`**, **`off`** oder **`false`**, um ihn zu deaktivieren.

Tabelle B.6. IP-Adresse (`ip`-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
IP Address, Netmask Bits	**address**	Die IP-Adresse (und optionale Netzmaskenbits) für die Ressource. Netzmaskenbits, oder Netzwerk-Präfixlänge, kann nach der Adresse selbst kommen, mit einem Schrägstrich als Trennzeichen, damit die CIDR-Notation (z. B. 10.1.1.1 / 8) eingehalten wird. Dies ist eine virtuelle IP-Adresse. IPv4-und IPv6-Adressen werden unterstützt, sowie NIC Link-Überwachung für jede IP-Adresse.
Monitor Link	**monitor_link**	Ist dies aktiviert, schlägt die Statusüberprüfung fehl, falls der Link auf der NIC, an die diese IP-Adresse gebunden ist, nicht vorhanden ist.
Disable Updates to Static Routes	**disable_rdisc**	Deaktiviert das Aktualisieren vom Routing mithilfe des RDISC-Protokolls.
Number of Seconds to Sleep After Removing an IP Address	**sleeptime**	Spezifiziert die Zeitspanne (in Sekunden) der Inaktivität.

Tabelle B.7. HA LVM (`lvm`-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Ein eindeutiger Name für diese LVM-Ressource.
Volume Group Name	**vg_name**	Ein beschreibender Name der verwalteten Datenträgergruppe.
Logical Volume Name	**lv_name**	Name des verwalteten logischen Datenträgers. Dieser Parameter ist optional, falls es mehr als einen logischen Datenträger in der verwalteten Datenträgergruppe gibt.
Fencing des Knotens, wenn er nicht in der Lage ist, LVM-Tags zu bereinigen	**self_fence**	Fencing des Knotens, wenn er nicht in der Lage ist, LVM-Tags zu bereinigen. Der LVM-Ressourcen-Agent akzeptiert die Werte 1 oder **yes**, um diesen Parameter zu aktivieren, und die Werte 0 oder **no**, um ihn zu deaktivieren.

Tabelle B.8. MySQL (`mysql`-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**`name`**	Spezifiziert einen Namen für die MySQL-Serverressource.
Config File	**`config_file`**	Spezifiziert die Konfigurationsdatei. Der Standardwert ist **`/etc/my.cnf`**.
Listen Address	**`listen_address`**	Spezifiziert eine IP-Adresse für MySQL-Server. Wird keine IP-Adresse angegeben, wird die erste IP-Adresse des Dienstes verwendet.
mysqld Options	**`mysqld_options`**	Weitere Befehlszeilenoptionen für **`mysqld`**.
Startup Wait (seconds)	**`startup_wait`**	Spezifiziert die Anzahl von Sekunden, die auf das korrekte Starten eines Dienstes gewartet wird.
Shutdown Wait (seconds)	**`shutdown_wait`**	Spezifiziert die Anzahl von Sekunden, die auf das korrekte Beenden eines Dienstes gewartet wird.

Tabelle B.9. NFS/CIFS Mount (`netfs`-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**`name`**	Symbolischer Name für den NFS- oder CIFS-Mount. **Anmerkung** Diese Ressource ist nur dann nötig, wenn ein Cluster-Dienst als NFS-Client konfiguriert wird.
Mount Point	**`mountpoint`**	Der Pfad, unter dem diese Dateisystemressource eingehängt wird.
Host	**`host`**	IP-Adresse oder Hostname des NFS/CIFS-Servers.
Name des NFS-Export-Verzeichnisses oder CIFS-Shares.	**`export`**	Name des NFS-Export-Verzeichnisses oder CIFS-Shares.
Filesystem Type	**`fstype`**	Dateisystemtyp: • ***`NFS`*** — Spezifiziert die Verwendung der standardmäßigen NFS-Version. Dies ist die Standardeinstellung. • ***`NFS v4`*** — Spezifiziert die Verwendung des NFSv4-Protokolls. • ***`CIFS`*** — Spezifiziert die Verwendung des CIFS-Protokolls.
Do Not Unmount the Filesystem During a Stop of Relocation Operation.	**`no_unmount`**	Falls aktiviert, wird das Dateisystem während einer Stopp- oder Verlegungs-Operation nicht ausgehängt.
Force Unmount	**`force_unmount`**	Falls ***`Force Unmount`*** aktiviert ist, vernichtet der Cluster beim Stoppen des Dienstes sämtliche Prozesse, die den Einhängepunkt verwenden, damit das eingehängte Dateisystem beim Aushängen nicht mehr verwendet wird. Andernfalls würde das Aushängen fehlschlagen und der Dienst würde neu gestartet werden.
Options	**`options`**	Einhängeoptionen. Spezifiziert eine Liste mit Einhängeoptionen. Werden keine angegeben, wird das Dateisystem mit **`-o sync`** eingehängt.

Tabelle B.10. NFS Client (`nfsclient`-Ressource)

luci-Feld	`cluster.conf` Parameter	Beschreibung
Name	**`name`**	Dies ist ein symbolischer Name für einen Client, der zur Referenzierung im Ressourcenbaum verwendet wird. Dies ist *nicht* dasselbe wie die ***`Target`*** Option.
Target Hostname, Wildcard, or Netgroup	**`target`**	Dies ist der Server von dem aus Sie einhängen. Er kann mittels Hostname, Platzhalter (basierend auf IP-Adresse oder Hostname) oder einer Netzgruppe spezifiziert werden, um Hosts zu definieren, auf die exportiert wird.
Allow Recovery of This NFS Client	**`allow_recover`**	Erlaubt die Wiederherstellung.
Options	**`options`**	Definiert eine Liste von Optionen für diesen Client — z.B. zusätzliche Client-Zugriffsrechte. Für weitere Informationen siehe die ***`exports`*** *(5)* Handbuchseite, *General Options*.

Tabelle B.11. NFS v3 Export (`nfsexport`-Ressource)

luci-Feld	`cluster.conf` Parameter	Beschreibung
Name	**`name`**	Beschreibender Name der Ressource. Die NFS-Export-Ressource gewährleistet, dass NFS-Daemons laufen. Sie ist voll wiederverwendbar; normalerweise ist nur eine NFS-Export-Ressource nötig. Weitere Informationen über die Konfiguration der **`nfsexport`**-Ressource finden Sie in Abschnitt 7.8, „Konfiguration von nfsexport- und nfsserver-Ressourcen“. **Tipp** Benennen Sie die NFS-Export-Ressource so, dass sie deutlich von anderen NFS-Ressourcen zu unterscheiden ist.

Tabelle B.12. NFS Server (`nfsserver`-Ressource)

luci-Feld	`cluster.conf` Parameter	Beschreibung
Name	**`name`**	Beschreibender Name der NFS-Server-Ressource. Die NFS-Server-Ressource ist nützlich für den Export von NFSv4-Dateisystemen zu Kunden. Aufgrund der Art und Weise, wie NFSv4 funktioniert, kann nicht mehr als eine NFSv4-Ressource auf einem Server gleichzeitig existieren. Darüber hinaus ist es nicht möglich, die NFS-Server-Ressource zu benutzen, wenn gleichzeitig lokale Instanzen von NFS auf jedem Cluster-Knoten verwendet werden. Weitere Informationen über die Konfiguration der **`nfsserver`**-Ressource finden Sie in Abschnitt 7.8, „Konfiguration von nfsexport- und nfsserver-Ressourcen“.

Tabelle B.13. Open LDAP (openldap-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	name	Spezifiziert einen Dienstnamen zur Protokollierung und zu anderen Zwecken.
Config File	config_file	Spezifiziert einen absoluten Pfad zu einer Konfigurationsdatei. Der Standardwert ist /etc/openldap/slapd.conf.
URL List	url_list	Der Standardwert ist ldap:///.
slapd Options	slapd_options	Weitere Befehlszeilenoptionen für slapd.
Shutdown Wait (seconds)	shutdown_wait	Spezifiziert die Anzahl von Sekunden, die auf das korrekte Beenden eines Dienstes gewartet wird.

Tabelle B.14. Oracle 10g/11g Ausfallsicherungsginstanz (oracledb-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Instance Name (SID) of Oracle Instance	name	Instanzenname.
Oracle Listener Instance Name	listener_name	Oracle-Listener-Instanzenname. Falls Sie mehrere Oracle-Instanzen ausführen, kann es nötig sein, mehrere Listeners mit verschiedenen Namen auf demselben Rechner auszuführen.
Oracle User Name	user	Dies ist der Benutzername des Oracle-Benutzers, in dessen Namen die Oracle AS-Instanz ausgeführt wird.
Oracle Application Home Directory	home	Dies ist das Benutzerverzeichnis von Oracle (der Applikation, nicht des Benutzers). Es wird bei der Installation von Oracle konfiguriert.
Oracle Installation Type	type	Der Oracle-Installationstyp. • Standard: 10g • base: Nur Datenbank-Instanz und Listener • base-11g: Nur Oracle11g Datenbank-Instanz und Listener • base-em (oder 10g): Datenbank, Listener, Enterprise Manager und iSQL*Plus • base-em-11g: Datenbank, Listener, Enterprise Manager dbconsole • ias (oder 10g-ias): Internet-Applikationsserver (Infrastruktur)
Virtual Hostname (optional)	vhost	Der virtuelle Hostname, der dem Installations-Hostnamen von Oracle 10g entspricht. Beachten Sie, dass Ihr Hostname beim Start/Stopp einer oracledb-Ressource vorübergehend auf diesen Hostnamen geändert wird. Deshalb sollten Sie eine oracledb-Ressource nur als Teil eines exklusiven Dienstes konfigurieren.
TNS_ADMIN (optional)	tns_admin	Pfad zur spezifischen Listener-Konfigurationsdatei

Tabelle B.15. Oracle 10g/11g Ausfallsicherungsinstanz (`orainstance`-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Instance name (SID) of Oracle instance	**name**	Instanzenname.
Oracle User Name	**user**	Dies ist der Benutzername des Oracle-Benutzers, in dessen Namen die Oracle-Instanz ausgeführt wird.
Oracle Application Home Directory	**home**	Dies ist das Benutzerverzeichnis von Oracle (der Applikation, nicht des Benutzers). Es wird bei der Installation von Oracle konfiguriert.
List of Oracle Listeners (optional, durch Leerzeichen getrennt)	**listeners**	Liste der Oracle-Listeners, die mit der Datenbankinstanz gestartet werden. Listener-Namen werden durch Leerzeichen voneinander getrennt.
Path to Lock File (optional)	**lockfile**	Speicherort der Sperrdatei, anhand derer festgestellt wird, ob Oracle laufen soll oder nicht. Standardmäßig ein Speicherort unter **/tmp**.
TNS_ADMIN (optional)	**tns_admin**	Pfad zur spezifischen Listener-Konfigurationsdatei

Tabelle B.16. Oracle 10g/11g Listener (`oralistener`-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Listener Name	**name**	Listener-Name.
Oracle User Name	**user**	Dies ist der Benutzername des Oracle-Benutzers, in dessen Namen die Oracle-Instanz ausgeführt wird.
Oracle Application Home Directory	**home**	Dies ist das Benutzerverzeichnis von Oracle (der Applikation, nicht des Benutzers). Es wird bei der Installation von Oracle konfiguriert.
TNS_ADMIN (optional)	**tns_admin**	Pfad zur spezifischen Listener-Konfigurationsdatei

Tabelle B.17. PostgreSQL 8 (`postgrest-8`-Ressource)

luci-Feld	`cluster.conf` Parameter	Beschreibung
Name	`name`	Spezifiziert einen Dienstnamen zur Protokollierung und zu anderen Zwecken.
Config File	`config_file`	Definiert einen absoluten Pfad zur Konfigurationsdatei. Der Standardwert ist `/var/lib/pgsql/data/postgresql.conf`.
Postmaster User	`postmaster_user`	Benutzer, der den Datenbank-Server ausführt, da dieser nicht von Root ausgeführt werden kann. Der Standardwert ist postgres.
Postmaster Options	`postmaster_options`	Weitere Befehlszeilenoptionen für Postmaster.
Shutdown Wait (seconds)	`shutdown_wait`	Spezifiziert die Anzahl von Sekunden, die auf das korrekte Beenden eines Dienstes gewartet wird.

Tabelle B.18. SAP-Datenbank (SAPDatabase-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
SAP Database Name	**SID**	Spezifiziert eine eindeutige SAP-Systemkennung, z.B. P01.
SAP Executable Directory	**DIR_EXECUTABLE**	Spezifiziert den voll qualifizierten Pfad zu **sapstartsrv** und **sapcontrol**.
Database Type	**DBTYPE**	Spezifiziert eine der folgenden Datenbanktypen: Oracle, DB6 oder ADA.
Oracle Listener Name	**NETSERVICENAME**	Spezifiziert den Oracle TNS Listener-Name.
ABAP Stack is Not Installed, Only Java Stack is Installed	**DBJ2EE_ONLY**	Falls Sie keinen ABAP-Stapel in der SAP-Datenbank installiert haben, aktivieren Sie diesen Parameter.
Application Level Monitoring	**STRICT_MONITORING**	Aktiviert die Überwachung auf Applikationsebene.
Automatic Startup Recovery	**AUTOMATIC_RECOVER**	Aktiviert bzw. deaktiviert automatische Startup-Recovery.
Path to Java SDK	**JAVE_HOME**	Pfad zur Java SDK.
File Name of the JDBC Driver	**DB_JARS**	Dateiname des JDBC-Treibers.
Path to a Pre-Start Script	**PRE_START_USEREXIT**	Pfad zu einem Prä-Start-Skript.
Path to a Post-Start Script	**POST_START_USEREXIT**	Pfad zu einem Post-Start-Skript.
Path to a Pre-Stop Script	**PRE_STOP_USEREXIT**	Pfad zu einem Prä-Stop-Skript.
Path to a Post-Stop Script	**POST_STOP_USEREXIT**	Pfad zu einem Post-Stop-Skript.
J2EE Instance Bootstrap Directory	**DIR_BOOTSTRAP**	Der voll qualifizierte Pfad des Bootstrap-Verzeichnisses der J2EE-Instanz, z.B. **/usr/sap/P01/J00/j2ee/cluster/bootstrap**.
J2EE Security Store Path	**DIR_SECSTORE**	Der voll qualifizierte Pfad des J2EE-Sicherheitsspeicher-Verzeichnisses, z.B. **/usr/sap/P01/SYS/global/security/lib/tools**.

Tabelle B.19. SAP-Instanz (SAPInstance-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
SAP Instance Name	**InstanceName**	Der vollqualifizierte Name der SAP-Instanz, z.B. P01_DVEBMGS00_sapp01ci.
SAP Executable Directory	**DIR_EXECUTABLE**	Der vollqualifizierte Pfad zu **sapstartsrv** und **sapcontrol**.
Directory Containing the SAP START Profile	**DIR_PROFILE**	Der vollqualifizierte Pfad zum SAP START Profil.
Name of the SAP START Profile	**START_PROFILE**	Spezifiziert den Namen des SAP START Profils.
Number of Seconds to Wait Before Checking Startup Status	**START_WAITTIME**	Spezifiziert die Anzahl von Sekunden, bevor der Status des Starts überprüft wird (nicht auf J2EE-Addin warten).
Enable Automatic Startup Recovery	**AUTOMATIC_RECOVER**	Aktiviert bzw. deaktiviert automatische Startup-Recovery.
Path to a Pre-Start Script	**PRE_START_USEREXIT**	Pfad zu einem Prä-Start-Skript.
Path to a Post-Start Script	**POST_START_USEREXIT**	Pfad zu einem Post-Start-Skript.
Path to a Pre-Stop Script	**PRE_STOP_USEREXIT**	Pfad zu einem Prä-Stop-Skript.
Path to a Post-Stop Script	**POST_STOP_USEREXIT**	Pfad zu einem Post-Stop-Skript.



Anmerkung

Zu Tabelle B.20, „Samba-Server (**samba**-Ressource)“: Beim Erstellen oder Ändern eines Cluster-Dienstes sollten Sie eine Samba-Dienst Ressource direkt mit dem Dienst verbinden, *nicht* mit einer Ressource innerhalb eines Dienstes.

Tabelle B.20. Samba-Server (samba-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	`name`	Spezifiziert den Namen des Samba-Servers.
Config File	`config_file`	Die Samba-Konfigurationsdatei
Other Command-Line Options for smbd	`smbd_options`	Andere Befehlszeilenoptionen für smbd.
Other Command-Line Options for nmbd	`nmbd_options`	Andere Befehlszeilenoptionen für nmbd.
Shutdown Wait (seconds)	`shutdown_wait`	Spezifiziert die Anzahl von Sekunden, die auf das korrekte Beenden eines Dienstes gewartet wird.

Tabelle B.21. Skript (script-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	`name`	Spezifiziert einen Namen für das benutzerdefinierte Benutzerskript. Die Skriptressource ermöglicht es Ihnen, für den Start eines geclusterten Dienstes ein standardmäßiges, LSB-konformes init-Skript zu verwenden.
Full Path to Script File	`file`	Geben Sie den Pfad an, auf dem sich dieses benutzerdefinierte Skript befindet (z.B. **/etc/init.d/*userscript***).

Tabelle B.22. Sybase ASE Ausfallsicherungsinstanz (ASEHAagent-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Instance Name	**name**	Spezifiziert den Instanzennamen der Sybase ASE-Ressource.
ASE Server Name	**server_name**	Der ASE-Servername, der für den Hochverfügbarkeitsdienst konfiguriert ist.
SYBASE Home directory	**sybase_home**	Das Benutzerverzeichnis für Sybase-Produkte.
Login File	**login_file**	Der vollständige Pfad zur Login-Datei, die das Login-Passwort-Paar enthält.
Interfaces File	**interfaces_file**	Der vollständige Pfad zur Schnittstellendatei, die zum Starten und zum Zugriff auf den ASE-Server verwendet wird.
SYBASE_ASE Directory Name	**sybase_ase**	Der Verzeichnisname unter sybase_home, wo ASE-Produkte installiert werden.
SYBASE_OCS Directory Name	**sybase_ocs**	Der Verzeichnisname unter sybase_home, wo OCS-Produkte installiert werden, z.B. ASE-15_0.
Sybase User	**sybase_user**	Der Benutzer, der den ASE-Server ausführen kann.
Start Timeout (seconds)	**start_timeout**	Der Start-Timeoutwert.
Shutdown Timeout (seconds)	**shutdown_timeout**	Der Beenden-Timoutwert.
Deep Probe Timeout	**deep_probe_timeout**	Die maximale Anzahl von Sekunden, die auf eine Antwort vom ASE-Server gewartet wird, bevor davon ausgegangen wird, dass der Server während der Deep-Probe keine Antwort erhalten hat.

Tabelle B.23. Tomcat 6 (tomcat-6-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Name	**name**	Spezifiziert einen Dienstnamen zur Protokollierung und zu anderen Zwecken.
Config File	**config_file**	Spezifiziert den absoluten Pfad zu einer Konfigurationsdatei. Der Standardwert lautet **/etc/tomcat6/tomcat6.conf**.
Shutdown Wait (seconds)	**shutdown_wait**	Spezifiziert die Anzahl von Sekunden, die auf das korrekte Beenden eines Dienstes gewartet wird. Der Standardwert ist 30.



Wichtig

Zu Tabelle B.24, „Virtuelle Maschine (vm-Ressource)“: Wenn Sie Ihren Cluster mit virtuellen Maschinen-Ressourcen konfigurieren, sollten Sie die **rgmanager** Tools benutzen, um die virtuellen Maschinen zu starten und zu stoppen. Wenn Sie dagegen **virsh** zum Starten der Maschine benutzen, kann es passieren, dass die virtuelle Maschine an mehr als einem Ort ausgeführt wird, was wiederum zur Beschädigung von Daten in der virtuellen Maschine führen kann. Siehe Abschnitt 2.14, „Konfiguration von virtuellen Maschinen in einer Cluster-Umgebung“ für Informationen darüber, wie Ihr System konfiguriert werden kann, um die Wahrscheinlichkeit zu verringern, dass Administratoren versehentlich virtuelle Maschinen mehrfach mit Cluster- und Non-Cluster-Tools starten.



Anmerkung

Virtuelle Maschinen-Ressourcen werden anders konfiguriert als andere Cluster-Ressourcen. Um eine virtuelle Maschinen-Ressource mit **luci** zu konfigurieren, fügen Sie eine Dienstgruppe zum Cluster hinzu, fügen Sie anschließend eine Ressource zum Dienst hinzu, wobei Sie **`Virtual Machine`** als Ressourcentyp wählen, und geben Sie die Parameter der virtuellen Maschinen-Ressource an. Für Informationen über das Konfigurieren einer virtuellen Maschine mit **`ccs`** siehe Abschnitt 5.12, „Virtuelle Maschinen-Ressourcen“ .

Tabelle B.24. Virtuelle Maschine (vm-Ressource)

luci-Feld	cluster.conf Parameter	Beschreibung
Service Name	**name**	Spezifiziert den Namen der virtuellen Maschine. Wenn Sie die **Luci** Oberfläche verwenden, spezifizieren Sie dies als den Dienstnamen.
Automatically Start This Service	**autostart**	Falls aktiviert, wird diese virtuelle Maschine automatisch gestartet, sobald der Cluster ein Quorum bildet. Ist dieser Parameter *disabled*, startet diese virtuelle Maschine *nicht* automatisch, sobald der Cluster ein Quorum bildet; die virtuelle Maschine wird in den ***disabled*** Status versetzt.
Run Exclusive	**exclusive**	Falls aktiviert, kann diese virtuelle Maschine nur verlegt werden, wenn sie auf dem anderen Knoten exklusiv läuft; sie kann also nur auf einen Knoten verlegt werden, auf dem keine anderen virtuellen Maschinen ausgeführt werden. Falls keine Knoten zur Verfügung stehen, die eine virtuelle Maschine exklusiv ausführen könnten, wird diese virtuelle Maschine nach einem Ausfall nicht wieder gestartet. Außerdem werden andere virtuelle Maschinen nicht automatisch auf einen Knoten verlegt, der diese virtuelle Maschine als ***Run exclusive*** ausführt. Sie können diese Option mithilfe manueller Start- oder Verlegungsoperationen außer Kraft setzen.
Failover Domain	**domain**	Definiert eine Liste mit Cluster-Mitgliedern, die im Falle eines Ausfalls der virtuellen Maschine ersatzweise versucht werden sollen.
Recovery Policy	**recovery**	***Recovery policy*** bietet die folgenden Optionen: » ***Disable*** — Deaktiviert die virtuelle Maschine, falls diese ausfällt. » ***Relocate*** — Versucht, die virtuelle Maschine auf einem anderen Knoten zu starten, anstatt zu versuchen, sie auf dem derzeitigen Knoten neu zu starten. » ***Restart*** — Versucht, die virtuelle Maschine lokal (auf dem derzeitigen Knoten) neu zu starten, bevor versucht wird, sie auf einen anderen Knoten zu verlegen (Standard). » ***Restart-Disable*** — Der Dienst wird nach einem Ausfall an derselben Stelle neu gestartet. Falls der Neustart jedoch fehlschlägt, wird der Dienst nicht auf einen anderen Host im Cluster verlegt, sondern deaktiviert.
Restart Options	**max_restarts**, **restart_expire_time**	Falls Sie **Restart** oder **Restart-Disable** als Wiederherstellungsrichtlinie für einen Dienst auswählen, können Sie die maximale Anzahl an Neustartfehlschlägen festlegen, bevor der Dienst verlegt oder deaktiviert wird, sowie die Zeitspanne in Sekunden, nach der ein Neustart nicht weiter versucht werden soll.
Migration Type	**migrate**	Spezifiziert den Migrationstyp ***live*** oder ***pause***. Die Standardeinstellung ist ***live***.
Migration Mapping	**migration_mapping**	Spezifiziert eine alternative Schnittstelle für die Migration. Sie können dies beispielsweise festlegen, wenn sich die Netzwerkadresse für die Migration der virtuellen Maschine eines Knotens von der Adresse des Knotens für die Cluster-Kommunikation unterscheidet. Folgende Angaben führen dazu, dass Sie beim Migrieren einer virtuellen Maschine von **member** nach **member2** tatsächlich nach **target2** migrieren. Wenn Sie von **member2** nach **member**

		migrieren, wird **target** zur Migration verwendet. **member:target,member2:target2**
Status Program	**status_program**	Das auszuführende Statusprogramm, zusätzlich zur standardmäßigen Überprüfung auf virtuelle Maschinen. Falls spezifiziert, wird das Statusprogramm einmal pro Minute ausgeführt. Dies erlaubt Ihnen, den Status kritischer Dienste innerhalb einer virtuellen Maschine zu bestimmen. Wenn Ihre virtuelle Maschine beispielsweise einen Webserver ausführt, sollte Ihr Statusprogramm überprüfen, ob ein Webserver läuft; falls die Statusüberprüfung fehlschlägt (gekennzeichnet durch eine nicht-Null Ausgabe), wird die virtuelle Maschine wiederhergestellt. Nachdem eine virtuelle Maschine gestartet wurde, wird der Ressourcen-Agent der virtuellen Maschine regelmäßig das Statusprogramm ausführen und auf einen erfolgreichen Antwort-Code (Null) warten, bevor er zurückkehrt. Nach fünf Minuten erfolgt eine Zeitüberschreitung.
Path to xmlfile Used to Create the VM	**xmlfile**	Vollständiger Pfad zur **libvirt** XML-Datei, welche die **libvirt** Domain-Definition enthält.
VM Configuration File Path	**path**	Eine durch Doppelpunkt getrennte Pfadspezifikation, die der Ressourcen-Agent der virtuellen Maschine (**vm.sh**) nach der Konfigurationsdatei der virtuellen Maschine durchsucht. Zum Beispiel: **/mnt/guests/config:/etc/libvirt/qemu**. **Wichtig** Der Pfad sollte *nie* direkt auf eine Konfigurationsdatei einer virtuellen Maschine verweisen.
Path to the VM Snapshot Directory	**snapshot**	Pfad zum Snapshot-Verzeichnis, in dem das Image der virtuellen Maschinen gespeichert wird.
Hypervisor URI	**hypervisor_uri**	Hypervisor-URI (normalerweise automatisch).
Migration URI	**migration_uri**	Migrations-URI (normalerweise automatisch).
Tunnel data over ssh during migration	**tunnelled**	Daten bei der Migration über SSH tunneln.

Verhalten der Hochverfügbarkeitsressourcen

Dieser Anhang beschreibt das übliche Verhalten von Hochverfügbarkeitsressourcen. Es soll Ihnen ergänzende Informationen liefern, die Ihnen bei der Konfiguration von Hochverfügbarkeitsdiensten helfen können. Sie können die Parameter mithilfe von **luci** konfigurieren, oder indem Sie **`/etc/cluster/cluster.conf`** bearbeiten. Beschreibungen der Parameter der Hochverfügbarkeitsressourcen finden Sie in Anhang B, *Parameter der Hochverfügbarkeitsressourcen*. Für ein besseres Verständnis von Ressourcen-Agenten können Sie sich diese in **`/usr/share/cluster`** in jedem beliebigen Cluster-Knoten ansehen.



Anmerkung

Um die Informationen in diesem Anhang umfassend verstehen zu können, benötigen Sie u.U. ebenfalls ein gründliches Verständnis der Ressourcen-Agenten und der Cluster-Konfigurationsdatei **`/etc/cluster/cluster.conf`**.

Ein Hochverfügbarkeitsdienst besteht aus einer Gruppe von Cluster-Ressourcen, die als eine zusammenhängende Einheit konfiguriert wurden und zusammen einen spezialisierten Dienst für Clients bereitstellen. Ein Hochverfügbarkeitsdienst wird als Ressourcenbaum in der Cluster-Konfigurationsdatei **`/etc/cluster/cluster.conf`** dargestellt (in jedem Cluster-Knoten). In der Cluster-Konfigurationsdatei ist jeder Ressourcenbaum eine XML-Darstellung, die jede Ressource spezifiziert, deren Parameter, sowie ihre Relationen zu anderen Ressourcen im Ressourcenbaum (Eltern-, Kind-, Geschwisterrelationen).



Anmerkung

Da ein Hochverfügbarkeitsdienst aus Ressourcen besteht, die in einem hierarchischen Baum angeordnet sind, wird ein solcher Dienst manchmal auch als *Ressourcenbaum* oder *Ressourcen-Gruppe* bezeichnet. Beide Ausdrücke sind Synonyme für *Hochverfügbarkeitsdienst*.

An der Wurzel (Root) eines jeden Ressourcenbaums befindet sich eine besondere Art von Ressource — eine *Dienstressource*. Andere Arten von Ressourcen bilden den Rest eines Dienstes und bestimmen so dessen Charakteristiken. Zum Erstellen eines Hochverfügbarkeitsdienstes gehört das Erstellen einer Dienstressource, das Erstellen untergeordneter Cluster-Ressourcen, sowie deren Anordnung in eine zusammenhängende Einheit gemäß den hierarchischen Einschränkungen des Dienstes.

Dieser Anhang umfasst die folgenden Abschnitte:

- Abschnitt C.1, „Eltern-, Kind- und Geschwisterrelationen zwischen den Ressourcen“
- Abschnitt C.2, „Start-Reihenfolge von Kind- und Geschwisterressourcen“
- Abschnitt C.3, „Vererbung, der <resources> Block, und Wiederverwendung von Ressourcen“
- Abschnitt C.4, „Wiederherstellung nach Ausfall und unabhängige Unterbäume“
- Abschnitt C.5, „Testen und Fehlerbehebung von Diensten und der Ressourcenreihenfolge“



Anmerkung

Die folgenden Abschnitte zeigen Beispiele der Cluster-Konfigurationsdatei **`/etc/cluster/cluster.conf`**, die jedoch nur der Veranschaulichung dienen sollen.

C.1. Eltern-, Kind- und Geschwisterrelationen zwischen den Ressourcen

Ein Cluster-Dienst ist eine integrierte Einheit, die unter der Kontrolle von **`rgmanager`** läuft. Alle Ressourcen in einem Dienst laufen auf demselben Knoten. Aus Sicht des **`rgmanager`** ist ein Cluster-Dienst eine Einheit, die gestartet, gestoppt oder verlegt werden kann. Innerhalb eines Cluster-Dienstes bestimmt jedoch die Hierarchie der Ressourcen, in welcher Reihenfolge die Ressourcen gestartet und gestoppt werden. Die Hierarchie-Ebenen sind Eltern, Kinder und Geschwister.

Beispiel C.1, „Ressourcenhierarchie des Dienstes foo“ zeigt ein Beispiel für einen Ressourcenbaum des Dienstes *foo*. In diesem Beispiel stehen die Ressourcen wie folgt miteinander in Relation:

- **`fs:myfs`** (<fs name="myfs" ...>) und **`ip:10.1.1.2`** (<ip address="10.1.1.2 .../>) sind Geschwister.
- **`fs:myfs`** (<fs name="myfs" ...>) sind die Eltern von **`script:script_child`** (<script name="script_child"/>).
- **`script:script_child`** (<script name="script_child"/>) ist das Kind von **`fs:myfs`** (<fs name="myfs" ...>).

Beispiel C.1. Ressourcenhierarchie des Dienstes foo

```
<service name="foo" ...>
    <fs name="myfs" ...>
        <script name="script_child"/>
    </fs>
    <ip address="10.1.1.2" .../>
</service>
```

Die folgenden Regeln gelten für Eltern/Kind-Relationen in einem Ressourcenbaum:

- Eltern werden vor ihren Kindern gestartet.
- Kinder müssen alle sauber gestoppt worden sein, bevor die Eltern gestoppt werden dürfen.
- Damit eine Ressource als "gesund" betrachtet wird, müssen alle ihre Kinder ebenfalls "gesund" sein.



Anmerkung

Wenn Sie einen Abhängigkeitenbaum für einen Cluster-Dienst konfigurieren, der eine IP-Adress-Ressource enthält, deren IP-Adresse geändert werden darf ("Floating"), müssen Sie die IP-Ressource als ersten Eintrag konfigurieren und nicht als Kind einer anderen Ressource.

C.2. Start-Reihenfolge von Kind- und Geschwisterressourcen

Die Dienstressource bestimmt die Start- und Stopp-Reihenfolge einer Kindressource danach, ob diese einen Kind-Typ-Parameter für eine Kindressource kennzeichnet, und zwar wie folgt:

- Gekennzeichnet mit dem Kind-Typ-Parameter (*typisiert* als Kindressource) — Falls die Dienstressource eine Kindressource mit dem Kind-Typ-Parameter kennzeichnet, ist die Kindressource *typisiert*. Der Kind-Typ-Parameter bestimmt explizit die Start- und Stopp-Reihenfolge der Kindressource.
- *Nicht gekennzeichnet* mit dem Kind-Typ-Parameter (*nicht typisiert* als Kindressource) — Falls die Dienstressource eine Kindressource *nicht* mit dem Kind-Typ-Parameter kennzeichnet, ist die Kindressource *nicht typisiert*. Die Dienstressource steuert nicht explizit die Start- und Stopp-Reihenfolge einer nicht typisierten Kindressource. Allerdings wird eine nicht typisierte Kindressource gemäß der Reihenfolge in **`/etc/cluster/cluster.conf`** gestartet und gestoppt. Zudem werden nicht typisierte Kindressourcen gestartet, nachdem alle typisierten Kindressourcen gestartet wurden, und sie werden gestoppt, bevor jegliche typisierten Kindressourcen gestoppt werden.



Anmerkung

Die einzige Ressource, die eine Sortierung nach definierten *Kind-Ressourcentyp* implementiert, ist die Dienstressource.

Weitere Informationen über die Start-/Stopp-Reihenfolge von typisierten Kindressourcen finden Sie in Abschnitt C.2.1, „Start-/Stopp-Reihenfolge von typisierten Kindressourcen“. Weitere Informationen über die Start-/Stopp-Reihenfolge von nicht typisierten Kindressourcen finden Sie in Abschnitt C.2.2, „Start- und Stopp-Reihenfolge von nicht typisierten Kindressourcen“.

C.2.1. Start-/Stopp-Reihenfolge von typisierten Kindressourcen

Bei einer typisierten Kindressource definiert der Typ-Parameter der Kindressource die Start- und Stopp-Reihenfolge eines jeden Ressourcentyps mit einer Nummer zwischen 1 und 100; ein Wert für den Start, und ein Wert für den Stopp. Je niedriger die Nummer, desto früher wird ein Ressourcentyp gestartet oder gestoppt. Tabelle C.1, „Start-/Stopp-Reihenfolge von typisierten Kindressourcen“ zeigt beispielsweise die Start- und Stopp-Werte für jeden Ressourcentyp; Beispiel C.2, „Start und Stopp-Werte der Ressourcen: Auszug aus dem Dienstressourcen-Agent, **`service.sh`**“ zeigt die Start- und Stopp-Werte, wie sie im Dienstressourcen-Agenten, **`service.sh`**, erscheinen. Für die Dienstressource werden alle LVM-Kinder zuerst gestartet, gefolgt von allen Dateisystem-Kindern, wiederum gefolgt von allen Skript-Kindern, usw.

Tabelle C.1. Start-/Stopp-Reihenfolge von typisierten Kindressourcen

Ressource	Kindtyp	Start-Reihenfolge	Stopp-Reihenfolge
LVM	lvm	1	9
Dateisystem	fs	2	8
GFS2-Dateisystem	clusterfs	3	7
NFS-Mount	netfs	4	6
NFS-Export	nfsexport	5	5
NFS-Client	nfsclient	6	4
IP-Adresse	ip	7	2
Samba	smb	8	3
Skript	script	9	1

Beispiel C.2. Start und Stopp-Werte der Ressourcen: Auszug aus dem Dienstressourcen-Agent, `service.sh`

```
<special tag="rgmanager">
    <attributes root="1" maxinstances="1"/>
    <child type="lvm" start="1" stop="9"/>
    <child type="fs" start="2" stop="8"/>
    <child type="clusterfs" start="3" stop="7"/>
    <child type="netfs" start="4" stop="6"/>
    <child type="nfsexport" start="5" stop="5"/>
    <child type="nfsclient" start="6" stop="4"/>
    <child type="ip" start="7" stop="2"/>
    <child type="smb" start="8" stop="3"/>
    <child type="script" start="9" stop="1"/>
</special>
```

Die Reihenfolge innerhalb eines Ressourcentyps wird bewahrt, da sie in der Cluster-Konfigurationsdatei **`/etc/cluster/cluster.conf`** gespeichert wird. Sehen Sie sich zum Beispiel die Start- und Stopp-Reihenfolge der typisierten Kindressourcen in Beispiel C.3, „Reihenfolge innerhalb eines

Ressourcentyps“ an.

Beispiel C.3. Reihenfolge innerhalb eines Ressourcentyps

```
<service name="foo">
  <script name="1" .../>
  <lvm name="1" .../>
  <ip address="10.1.1.1" .../>
  <fs name="1" .../>
  <lvm name="2" .../>
</service>
```

Start-Reihenfolge von typisierten Kindressourcen

In Beispiel C.3, „Reihenfolge innerhalb eines Ressourcentyps“ werden die Ressourcen in der folgenden Reihenfolge gestartet:

1. **lvm:1** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuerst gestartet. **lvm:1** (**<lvm name="1" .../>**) ist die erste LVM-Ressource, die von allen LVM-Ressourcen als Erste gestartet wird, da dies die erste LVM-Ressource ist, die im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt wird.
2. **lvm:2** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuerst gestartet. **lvm:2** (**<lvm name="2" .../>**) wird nach **lvm:1** gestartet, da sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** nach **lvm:1** aufgeführt wird.
3. **fs:1** — Dies ist eine Dateisystem-Ressource. Falls es noch weitere Dateisystem-Ressourcen im Dienst *foo* gibt, so starten diese in der Reihenfolge, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden.
4. **ip:10.1.1.1** — Dies ist eine IP-Adress-Ressource. Falls es noch weitere IP-Adress-Ressourcen im Dienst *foo* gibt, so starten diese in der Reihenfolge, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden.
5. **script:1** — Dies ist eine Skriptressource. Falls es noch weitere Skriptressourcen im Dienst *foo* gibt, so starten diese in der Reihenfolge, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden.

Stopp-Reihenfolge von typisierten Kindressourcen

In Beispiel C.3, „Reihenfolge innerhalb eines Ressourcentyps“ werden die Ressourcen in der folgenden Reihenfolge gestoppt:

1. **script:1** — Dies ist eine Skriptressource. Falls es noch weitere Skriptressourcen im Dienst *foo* gibt, so werden diese in der umgekehrten Reihenfolge gestoppt, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden.
2. **ip:10.1.1.1** — Dies ist eine IP-Adress-Ressource. Falls es noch weitere IP-Adress-Ressourcen im Dienst *foo* gibt, so werden diese in der umgekehrten Reihenfolge gestoppt, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden.
3. **fs:1** — Dies ist eine Dateisystem-Ressource. Falls es noch weitere Dateisystem Ressourcen im *foo* gibt, so werden diese in der umgekehrten Reihenfolge gestoppt, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden.
4. **lvm:2** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuletzt gestoppt. **lvm:2** (**<lvm name="2" .../>**) wird vor **lvm:1** gestoppt; Ressourcen innerhalb einer Ressourcentyp-Gruppe werden in der umgekehrten Reihenfolge, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden, gestoppt.
5. **lvm:1** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuletzt gestoppt. **lvm:1** (**<lvm name="1" .../>**) wird nach **lvm:2** gestoppt; Ressourcen innerhalb einer

Ressourcentyp-Gruppe werden in der umgekehrten Reihenfolge, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden, gestoppt.

C.2.2. Start- und Stopp-Reihenfolge von nicht typisierten Kindressourcen

Weitere Überlegungen sind für nicht typisierte Kindressourcen erforderlich. Für eine nicht typisierte Kindressource ist die Start- und Stopp-Reihenfolge nicht ausdrücklich von der Dienstressource angegeben. Stattdessen werden Start- und Stopp-Reihenfolge nach der Reihenfolge der Kindressource in **/etc/cluster/cluster.conf** bestimmt. Darüber hinaus werden nicht typisierte Kindressourcen nach allen typisierten Kindressourcen gestartet und vor jeder typisierten Kindressourcen gestoppt.

Sehen Sie sich zum Beispiel die Start- und Stopp-Reihenfolge der nicht typisierten Kindressourcen in Beispiel C.4, „Nicht typisierte und typisierte Kindressource in einem Dienst“ an.

Beispiel C.4. Nicht typisierte und typisierte Kindressource in einem Dienst

```
<service name="foo">
  <script name="1" .../>
  <nontypedresource name="foo"/>
  <lvm name="1" .../>
  <nontypedresourcetwo name="bar"/>
  <ip address="10.1.1.1" .../>
  <fs name="1" .../>
  <lvm name="2" .../>
</service>
```

Start-Reihenfolge von nicht typisierten Kindressourcen

In Beispiel C.4, „Nicht typisierte und typisierte Kindressource in einem Dienst“ werden die Kindressourcen in der folgenden Reihenfolge gestartet:

1. **lvm:1** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuerst gestartet. **lvm:1** (**<lvm name="1" .../>**) ist die erste LVM-Ressource, die von allen LVM-Ressourcen als Erste gestartet wird, da dies die erste LVM-Ressource ist, die im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt wird.
2. **lvm:2** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuerst gestartet. **lvm:2** (**<lvm name="2" .../>**) wird nach **lvm:1** gestartet, da sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** nach **lvm:1** aufgeführt wird.
3. **fs:1** — Dies ist eine Dateisystem-Ressource. Falls es noch weitere Dateisystem-Ressourcen im Dienst *foo* gibt, so starten diese in der Reihenfolge, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden.
4. **ip:10.1.1.1** — Dies ist eine IP-Adress-Ressource. Falls es noch weitere IP-Adress-Ressourcen im Dienst *foo* gibt, so starten diese in der Reihenfolge, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden.
5. **script:1** — Dies ist eine Skriptressource. Falls es noch weitere Skriptressourcen im Dienst *foo* gibt, so starten diese in der Reihenfolge, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden.
6. **nontypedresource:foo** — Dies ist eine nicht typisierte Ressource. Da es sich um eine nicht typisierte Ressource handelt, wird sie erst nach den typisierten Ressourcen gestartet. Zudem ist ihre Position in der Dienstressource vor der anderen nicht typisierten Ressource, **nontypedresourcetwo:bar**; daher wird sie noch vor **nontypedresourcetwo:bar** gestartet. (Nicht typisierte Ressourcen werden in der Reihenfolge gestartet, in der sie in der Dienstressource aufgeführt werden.)
7. **nontypedresourcetwo:bar** — Dies ist eine nicht typisierte Ressource. Da es sich um eine nicht typisierte Ressource handelt, wird sie erst nach den typisierten Ressourcen gestartet. Zudem ist ihre Position in der Dienstressource nach der anderen nicht typisierten Ressource,

nontypedresource:foo; daher wird sie nach **nontypedresource:foo** gestartet. (Nicht typisierte Ressourcen werden in der Reihenfolge gestartet, in der sie in der Dienstressource aufgeführt werden.)

Stopp-Reihenfolge von nicht typisierten Kindressourcen

In Beispiel C.4, „Nicht typisierte und typisierte Kindressource in einem Dienst“ werden die Kindressourcen in der folgenden Reihenfolge gestoppt:

1. **nontypedresourcetwo:bar** — Dies ist eine nicht typisierte Ressource. Da es sich um eine nicht typisierte Ressource handelt, wird sie vor den typisierten Ressourcen gestoppt. Zudem ist ihre Position in der Dienstressource nach der anderen nicht typisierten Ressource, **nontypedresource:foo**; daher wird sie vor **nontypedresource:foo** gestoppt. (Nicht typisierte Ressourcen werden in der umgekehrten Reihenfolge gestoppt, in der sie in der Dienstressource aufgeführt werden.)
2. **nontypedresource:foo** — Dies ist eine nicht typisierte Ressource. Da es sich um eine nicht typisierte Ressource handelt, wird sie vor den typisierten Ressourcen gestoppt. Zudem ist ihre Position in der Dienstressource vor der anderen nicht typisierten Ressource, **nontypedresourcetwo:bar**; daher wird sie nach **nontypedresourcetwo:bar** gestoppt. (Nicht typisierte Ressourcen werden in der umgekehrten Reihenfolge gestoppt, in der sie in der Dienstressource aufgeführt werden.)
3. **script:1** — Dies ist eine Skriptressource. Falls es noch weitere Skriptressourcen im Dienst *foo* gibt, so werden diese in der umgekehrten Reihenfolge gestoppt, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden.
4. **ip:10.1.1.1** — Dies ist eine IP-Adress-Ressource. Falls es noch weitere IP-Adress-Ressourcen im Dienst *foo* gibt, so werden diese in der umgekehrten Reihenfolge gestoppt, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden.
5. **fs:1** — Dies ist eine Dateisystem-Ressource. Falls es noch weitere Dateisystem Ressourcen im *foo* gibt, so werden diese in der umgekehrten Reihenfolge gestoppt, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden.
6. **lvm:2** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuletzt gestoppt. **lvm:2** (**<lvm name="2" .../>**) wird vor **lvm:1** gestoppt; Ressourcen innerhalb einer Ressourcentyp-Gruppe werden in der umgekehrten Reihenfolge, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden, gestoppt.
7. **lvm:1** — Dies ist eine LVM-Ressource. Alle LVM-Ressourcen werden zuletzt gestoppt. **lvm:1** (**<lvm name="1" .../>**) wird nach **lvm:2** gestoppt; Ressourcen innerhalb einer Ressourcentyp-Gruppe werden in der umgekehrten Reihenfolge, in der Sie im *foo* Dienstabschnitt von **/etc/cluster/cluster.conf** aufgeführt werden, gestoppt.

C.3. Vererbung, der <resources> Block, und Wiederverwendung von Ressourcen

Einige Ressourcen können davon profitieren, Werte von einer Elternressource zu erben; dies ist zum Beispiel üblicherweise bei einem NFS-Dienst der Fall. Beispiel C.5, „NFS-Dienst eingerichtet zur Ressourcen-Wiederverwendung und -Vererbung “ zeigt eine typische NFS-Dienstkonfiguration, die zur Ressourcen-Wiederverwendung und -Vererbung eingerichtet ist.

Beispiel C.5. NFS-Dienst eingerichtet zur Ressourcen-Wiederverwendung und -Vererbung

```
    <resources>
        <nfsclient name="bob" target="bob.example.com"
options="rw,no_root_squash"/>
        <nfsclient name="jim" target="jim.example.com"
options="rw,no_root_squash"/>
        <nfsexport name="exports"/>
    </resources>
    <service name="foo">
        <fs name="1" mountpoint="/mnt/foo" device="/dev/sdb1" fsid="12344">
            <nfsexport ref="exports">  <!-- nfsexport's path and fsid attributes
                                            are inherited from the mountpoint
&
                                            fsid attribute of the parent fs
                                            resource -->
                <nfsclient ref="bob"/> <!-- nfsclient's path is inherited from
the
                                            mountpoint and the fsid is added to
the
                                            options string during export -->
                <nfsclient ref="jim"/>
            </nfsexport>
        </fs>
        <fs name="2" mountpoint="/mnt/bar" device="/dev/sdb2" fsid="12345">
            <nfsexport ref="exports">
                <nfsclient ref="bob"/> <!-- Because all of the critical data
for this
                                            resource is either defined in the
                                            resources block or inherited, we
can
                                            reference it again! -->
                <nfsclient ref="jim"/>
            </nfsexport>
        </fs>
        <ip address="10.2.13.20"/>
    </service>
```

Wäre dieser Dienst flach (also ohne Eltern-/Kind-Relationen), müsste er wie folgt konfiguriert werden:

- Der Dienst benötigte vier nfsclient-Ressourcen — eine pro Dateisystem (insgesamt zwei für Dateisysteme), und eine pro Zielrechner (insgesamt zwei für Zielrechner).
- Der Dienst müsste den Exportpfad und die Dateisystem-ID für jeden nfsclient spezifizieren, was mögliche Fehlerquellen in die Konfiguration einbringt.

In Beispiel C.5, „NFS-Dienst eingerichtet zur Ressourcen-Wiederverwendung und -Vererbung“ werden die NFS-Client-Ressourcen *nfsclient:bob* und *nfsclient:jim* jedoch nur einmal definiert; ebenso wird die NFS-Export-Ressource *nfsexport:exports* nur einmal definiert. Alle von den Ressourcen benötigten Parameter werden von der Elternressource geerbt. Da die vererbten Parameter dynamisch sind (und nicht miteinander in Konflikt stehen), ist es möglich, diese Ressourcen wiederzuverwenden — weshalb sie im Ressourcenblock definiert sind. Es ist nicht sehr praktisch, manche Ressourcen an mehreren Stellen zu konfigurieren. Wenn Sie z.B. eine Dateisystemressource an mehreren Stellen konfigurieren, kann dies dazu führen, dass ein Dateisystem in zwei Knoten eingehängt wird und dadurch Probleme verursacht.

C.4. Wiederherstellung nach Ausfall und unabhängige Unterbäume

In den meisten Unternehmensumgebungen wird zur Wiederherstellung nach einem Dienstausfall in der

Regel der gesamte Dienst neu gestartet, auch wenn nur Teilkomponenten des Dienstes ausgefallen waren. Wenn in Beispiel C.6, „Dienst *foo* - Normale Wiederherstellung nach Ausfall“ z.B. eines der Skripte fehlschlägt, die in diesem Dienst definiert werden, so wird in der Regel der Dienst neu gestartet (oder verlegt oder deaktiviert, je nach Wiederherstellungsrichtlinie des Dienstes). In einigen Fällen können bestimmte Teile eines Dienstes als nicht-kritisch betrachtet werden; es kann notwendig sein, den Dienst nur in Teilen neu zu starten, bevor die normale Wiederherstellungsprozedur begonnen wird. Sie können zu diesem Zweck den ***__independent_subtree*** Parameter verwenden. In Beispiel C.7, „Dienst *foo* - Wiederherstellung nach Ausfall mit ***__independent_subtree*** Parameter“ wird der ***__independent_subtree*** Parameter verwendet, um die folgenden Aktionen durchzuführen:

- Falls script:script_one fehlschlägt, werden script:script_one, script:script_two und script:script_three neu gestartet.
- Falls script:script_two fehlschlägt, wird nur script:script_two neu gestartet.
- Falls script:script_three fehlschlägt, werden script:script_one, script:script_two und script:script_three neu gestartet.
- Falls script:script_four fehlschlägt, wird der gesamte Dienst neu gestartet.

Beispiel C.6. Dienst *foo* - Normale Wiederherstellung nach Ausfall

```
<service name="foo">
      <script name="script_one" ...>
          <script name="script_two" .../>
      </script>
      <script name="script_three" .../>
</service>
```

Beispiel C.7. Dienst *foo* - Wiederherstellung nach Ausfall mit *__independent_subtree* Parameter

```
<service name="foo">
      <script name="script_one" __independent_subtree="1" ...>
          <script name="script_two" __independent_subtree="1" .../>
          <script name="script_three" .../>
      </script>
      <script name="script_four" .../>
</service>
```

Unter Umständen möchten Sie beim Ausfall einer Dienstkomponente nur diese einzelne Komponente deaktivieren, ohne den gesamten Dienst zu deaktivieren, damit andere Dienste, die andere Komponenten dieses Dienstes nutzen, nicht ebenfalls in Mitleidenschaft gezogen werden. Ab der Red Hat Enterprise Linux 6.1 Release können Sie zu diesem Zweck den ***__independent_subtree="2"*** Parameter nutzen, der den unabhängigen Unterbaum als unkritisch kennzeichnet.



Anmerkung

Sie können die unkritisch-Flag nur auf Ressourcen mit einer einzigen Referenz anwenden. Das unkritisch-Flag funktioniert mit allen Ressourcen auf allen Ebenen des Ressourcenbaums, sollte jedoch nicht auf oberster Ebene angewendet werden, wenn Dienste oder virtuelle Maschinen definiert werden.

Ab der Red Hat Enterprise Linux 6.1 Release können Sie die maximalen Neustarts und den Neustart-Ablauf pro Knoten für unabhängige Unterbäume im Ressourcenbaum angeben. Um diese Grenzwerte einzustellen, verwenden Sie die folgenden Parameter:

- **`__max_restarts`** konfiguriert die Höchstanzahl der erlaubten Neustarts, bevor abgebrochen wird.
- **`__restart_expire_time`** konfiguriert die Zeitspanne in Sekunden, nach der kein Neustart mehr versucht wird.

C.5. Testen und Fehlerbehebung von Diensten und der Ressourcenreihenfolge

Sie können mithilfe des **`rg_test`** Dienstprogramms die Dienste und die Ressourcenreihenfolge testen und ggf. korrigieren. Bei **`rg_test`** handelt es sich um ein Befehlszeilen-Tool, das vom **`rgmanager`** Paket bereitgestellt wird, und von einer Shell oder einem Terminal ausgeführt wird (es ist nicht in **Conga** verfügbar). Tabelle C.2, „Übersicht über das **`rg_test`** Dienstprogramm“ fasst die Aktionen und die Syntax für das **`rg_test`** Dienstprogramm zusammen.

Tabelle C.2. Übersicht über das rg_test Dienstprogramm

Aktion	Syntax
Zeigt die Ressourcenregeln an, die **rg_test** versteht.	**rg_test rules**
Überprüft eine Konfiguration (und /usr/share/cluster) auf Fehler oder redundante Ressourcen-Agenten.	**rg_test test /etc/cluster/cluster.conf**
Zeigt die Start- und Stopp-Reihenfolge eines Dienstes.	Anzeige der Start-Reihenfolge: **rg_test noop /etc/cluster/cluster.conf start service *servicename*** Anzeige der Stopp-Reihenfolge: **rg_test noop /etc/cluster/cluster.conf stop service *servicename***
Startet oder stoppt einen Dienst explizit.	**Wichtig** Führen Sie dies nur auf einem Knoten aus und deaktivieren Sie den Dienst vorher grundsätzlich in rgmanager. Starten eines Dienstes: **rg_test test /etc/cluster/cluster.conf start service *servicename*** Stoppen eines Dienstes: **rg_test test /etc/cluster/cluster.conf stop service *servicename***
Berechnet und zeigt das Ressourcenbaum-Delta zwischen zwei cluster.conf-Dateien.	**rg_test delta *cluster.conf file 1* *cluster.conf file 2*** Zum Beispiel: **rg_test delta /etc/cluster/cluster.conf.bak /etc/cluster/cluster.conf**

Prüfung der Cluster-Dienstressource und Zeitüberschreitung der Ausfallsicherung

Dieser Anhang beschreibt, wie **rgmanager** den Status von Cluster-Ressourcen überwacht und wie die Zeitabstände der Statusprüfungen verändert werden können. Der Anhang beschreibt außerdem den **__enforce_timeouts** Dienstparameter, der festlegt, dass eine Zeitüberschreitung für eine Operation zum Fehlschlagen des Dienstes führen soll.



Anmerkung

Um die Informationen in diesem Anhang vollständig zu verstehen, benötigen Sie ein eingehendes Verständnis von Ressourcen-Agenten und der Cluster-Konfigurationsdatei **/etc/cluster/cluster.conf**. Eine vollständige Liste samt Beschreibung aller **cluster.conf**-Elemente und -Parameter finden Sie im Cluster-Schema unter **/usr/share/cluster/cluster.rng** und das kommentierte Schema unter **/usr/share/doc/cman-X.Y.ZZ/cluster_conf.html** (zum Beispiel **/usr/share/doc/cman-3.0.12/cluster_conf.html**).

D.1. Ändern des Intervalls zur Statusprüfung der Ressourcen

rgmanager prüft den Status einzelner Ressourcen, nicht ganzer Dienste. Alle 10 Sekunden prüft rgmanager den Ressourcenbaum und such nach Ressourcen, die ihren Intervall zur Statusprüfung überschritten haben.

Jeder Ressourcen-Agent spezifiziert die Zeitspanne zwischen den regelmäßigen Statusprüfungen. Jede Ressource benutzt diese Timeout-Werte, sofern diese nicht ausdrücklich in der **cluster.conf** Datei mit dem speziellen **<action>** Tag außer Kraft gesetzt werden:

```
<action name="status" depth="*" interval="10" />
```

Dieser Tag ist ein spezielles Unterelement der Ressource selbst in der **cluster.conf** Datei. Falls Sie beispielsweise eine Dateisystemressource haben, für die Sie den Statusprüfintervall ändern möchten, so können Sie die Dateisystemressource in der **cluster.conf** Datei wie folgt spezifizieren:

```
<fs name="test" device="/dev/sdb3">
  <action name="status" depth="*" interval="10" />
  <nfsexport...>
  </nfsexport>
</fs>
```

Einige Agenten bieten verschiedene "Tiefen" der Prüfung. Beispielsweise prüft eine normale Dateisystemstatusprüfung (Tiefe 0), ob das Dateisystem an der korrekten Stelle eingehängt ist. Eine intensivere Prüfung ist die Tiefe 10, bei der geprüft wird, ob Sie eine Datei vom Dateisystem lesen können. Eine Statusprüfung der Tiefe 20 prüft, ob Sie in das Dateisystem schreiben können. In dem vorliegenden Beispiel ist **depth** (Tiefe) auf ***** gesetzt, was bedeutet, dass diese Werte für alle Tiefen verwendet werden sollen. Infolgedessen wird das **test**-Dateisystem alle 10 Sekunden mit der höchsten definierten Tiefe des Ressourcen-Agenten geprüft (in diesem Fall 20).

D.2. Erzwingen von Ressourcen-Timeouts

Es gibt keinen Timeout beim Starten und Stoppen von Ressourcen oder bei der Ausfallsicherung. Einige Ressourcen brauchen eine unvorhersehbar lange Zeit zum Starten oder Stoppen. Unglücklicherweise wird durch einen Fehler beim Stoppen (inklusive Zeitüberschreitung) dieser Dienst unbenutzbar (Status

"fehlgeschlagen"). Falls gewünscht, können Sie auf jeder Ressource in einem Dienst einzeln das Erzwingen des Timeouts einstellen, indem Sie **`__enforce_timeouts="1"`** zur Referenz in der **`cluster.conf`**-Datei hinzufügen.

Das folgende Beispiel zeigt einen Cluster-Dienst, der mit dem **`__enforce_timeouts`** Parameter für die **`netfs`** Ressource konfiguriert wurde. Ist dieser Parameter gesetzt und das Aushängen des NFS-Dateisystems während eines Wiederherstellungsprozesses dauert mehr als 30 Sekunden, so erfolgt eine Zeitüberschreitung dieser Operation, wodurch der Dienst in den Status "fehlgeschlagen" eintritt.

```
</screen>
<rm>
  <failoverdomains/>
  <resources>
    <netfs export="/nfstest" force_unmount="1" fstype="nfs" host="10.65.48.65"
           mountpoint="/data/nfstest" name="nfstest_data" options="rw,sync,soft"/>
  </resources>
  <service autostart="1" exclusive="0" name="nfs_client_test" recovery="relocate">
    <netfs ref="nfstest_data" __enforce_timeouts="1"/>
  </service>
</rm>
```

Überblick über Befehlszeilen-Tools

Tabelle E.1, „Überblick über Befehlszeilen-Tools“ fasst die bevorzugten Befehlszeilen-Tools zur Konfiguration und zur Verwaltung des Hochverfügbarkeits-Add-Ons zusammen. Für weitere Informationen über Befehle und Variablen siehe die Handbuchseite des jeweiligen Befehlszeilen-Tools.

Tabelle E.1. Überblick über Befehlszeilen-Tools

Befehlszeilen-Tool	Verwendet mit	Zweck
ccs_config_dump — Tool zum Erstellen von Speicherauszügen der Cluster-Konfiguration	Cluster-Infrastruktur	**ccs_config_dump** generiert eine XML-Ausgabe der laufenden Konfiguration. Die laufende Konfiguration kann sich unter Umständen von der gespeicherten Konfiguration unterscheiden, da einige Untersysteme bestimmte Standardinformationen in der Konfiguration ablegen oder erstellen. Diese Werte sind in der Regel nicht in der auf der Festplatte gespeicherten Version der Konfiguration vorhanden, sind jedoch zur Laufzeit nötig, damit der Cluster ordnungsgemäß funktionieren kann. Weitere Informationen über dieses Tool finden Sie auf der ccs_config_dump(8) Handbuchseite.
ccs_config_validate — Tool zur Überprüfung der Cluster-Konfiguration	Cluster-Infrastruktur	**ccs_config_validate** überprüft **cluster.conf** anhand des Schemas **cluster.rng** (befindet sich in **/usr/share/cluster/cluster.rng** auf jedem Knoten). Weitere Informationen über dieses Tool finden Sie auf der ccs_config_validate(8) Handbuchseite.
clustat — Dienstprogramm zum Cluster-Status	Komponenten zur Verwaltung von Hochverfügbarkeitsdiensten	Der **clustat** Befehl zeigt den Status des Clusters an, einschließlich Mitgliedschaftsinformationen, Quorum-Ansicht, und dem Status aller konfigurierten Benutzerdienste. Weitere Informationen über dieses Tool finden Sie auf der clustat(8) Handbuchseite.
clusvcadm — Dienstprogramm zur Cluster-Benutzerdienstverwaltung	Komponenten zur Verwaltung von Hochverfügbarkeitsdiensten	Der **clusvcadm** Befehl ermöglicht Ihnen das Aktivieren, Deaktivieren, Verlegen und Neustarten von Hochverfügbarkeitsdiensten in einem Cluster. Weitere Informationen über dieses Tool finden Sie auf der clusvcadm(8) Handbuchseite.
cman_tool — Tool zur Cluster-Verwaltung	Cluster-Infrastruktur	**cman_tool** ist ein Programm, das den CMAN Cluster-Manager verwaltet. Es bietet die Funktionalität, um einem Cluster beizutreten, einen Cluster zu verlassen, einen Knoten abzubrechen, oder die erwarteten Quorum-Stimmen in einem Cluster zu ändern. Weitere Informationen über dieses Tool finden Sie auf der cman_tool(8) Handbuchseite.
fence_tool — Fencing-Tool	Cluster-Infrastruktur	**fence_tool** ist ein Programm, das zum Beitreten oder Verlassen einer Fencing-Domain verwendet wird. Weitere Informationen über dieses Tool finden Sie auf der fence_tool(8) Handbuchseite.

High Availability LVM (HA-LVM)

Das Red Hat Hochverfügbarkeits-Add-On bietet Unterstützung für hochverfügbare LVM-Datenträger (HA-LVM) in einer Ausfallsicherungs-Konfiguration. Dies unterscheidet sich von active/active-Konfigurationen mithilfe des Clustered Logical Volume Manager (CLVM), bei dem es sich um eine Reihe von Clustering-Erweiterungen zu LVM handelt, die einem Cluster von Computern die Verwaltung von gemeinsam genutztem Speicher erlauben.

Die Entscheidung, ob CLVM oder HA-LVM eingesetzt werden sollte, hängt von den Anforderungen der implementierten Applikationen oder Dienste ab.

- Falls die Applikationen clusterfähig sind und zur simultanen Ausführung auf mehreren Rechnern optimiert wurden, dann sollte CLVM verwendet werden. Insbesondere müssen Sie CLVM einsetzen, falls mehr als ein Knoten in Ihrem Cluster Zugriff auf den Speicher benötigt, der somit also von den aktiven Knoten gemeinsam verwendet wird. CLVM ermöglicht einem Benutzer die Konfiguration von logischen Datenträgern auf gemeinsam genutztem Speicher, indem der Zugriff auf den physischen Speicher während der Konfiguration des logischen Datenträgers gesperrt wird, und verwendet geclusterte Sperrdienste, um den gemeinsam verwendeten Speicher zu verwalten. Für weitere Informationen über CLVM und über die LVM-Konfiguration im Allgemeinen siehe *Logical Volume Manager Administration*.
- Falls die Applikationen optimal in active/passive-Konfigurationen (Ausfallsicherung) laufen, in denen zu jeder Zeit nur ein Knoten aktiv ist, der auf den Speicher zugreift, sollten Sie High Availability Logical Volume Management Agenten (HA-LVM) einsetzen.

Die meisten Applikationen laufen besser in einer active/passive-Konfiguration, da sie für die gleichzeitige Ausführung mit anderen Instanzen weder ausgelegt noch optimiert sind. Wenn Sie eine Applikation, die nicht clusterfähig ist, auf geclusterten logischen Datenträgern ausführen, kann dies zu eingeschränkter Leistung führen, falls der logische Datenträger gespiegelt wird. Der Grund dafür ist in diesen Instanzen der Mehraufwand durch die Cluster-Kommunikation der logischen Datenträger selbst. Eine clusterfähige Applikation muss dazu in der Lage sein, Leistungsvorteile zu erreichen, die die Leistungseinbußen durch die Cluster-Dateisysteme und clusterfähigen logischen Datenträger aufwiegen. Für einige Applikationen und Arbeitslasten ist dies einfacher zu erreichen als für andere. Für die Entscheidung zwischen den zwei LVM-Varianten müssen Sie daher die Anforderungen an den Cluster definieren und abwägen, ob der zusätzliche Aufwand für die Optimierung für eine active/active-Konfiguration die möglichen Vorteile rechtfertigt. Die meisten Benutzer werden die besten HA-Ergebnisse mit HA-LVM erreichen.

HA-LVM und CLVM ähneln sich insofern, als sie die Beschädigung von LVM-Metadaten und den logischen Datenträgern verhindern, die andernfalls auftreten könnte, falls mehrere Rechner sich überschneidende Änderungen vornehmen dürften. HA-LVM erzwingt, dass ein logischer Datenträger nur exklusiv aktiviert werden kann, mit anderen Worten, zu jeder Zeit nur auf einem Rechner aktiv sein kann. Das bedeutet, dass nur die lokalen (nicht geclusterten) Implementierungen der Speichertreiber verwendet werden. Indem auf diese Weise der Mehraufwand der Cluster-Koordination vermieden wird, steigt die Leistung. CLVM hat diese Einschränkungen nicht - ein Benutzer kann nach Belieben einen logischen Datenträger auf allen Rechnern im Cluster aktivieren; dies erfordert die Verwendung von clusterfähigen Speichertreibern, die es ermöglichen, clusterfähige Dateisysteme und darauf Applikationen zu betreiben.

HA-LVM kann mit zwei verschiedenen Methoden eingerichtet werden, um das exklusive Aktivieren logischer Datenträger zu erreichen.

- Die bevorzugte Methode benutzt CLVM, aktiviert die logischen Datenträger jedoch immer nur exklusiv. Dies hat den Vorteil, dass es einfacher einzurichten ist und dass administrative Fehler (wie das Entfernen eines derzeit verwendeten logischen Datenträgers) vermieden werden. Um CLVM zu verwenden, muss die Hochverfügbarkeits-Add-On und Resilient Storage Add-On Software einschließlich des **`clvmd`** Daemons laufen.

  Das Verfahren zur Konfiguration von HA-LVM mithilfe dieser Methode wird in Abschnitt F.1, „Konfiguration von HA-LVM-Ausfallsicherung mit CLVM (bevorzugt)“ beschrieben.
- Die zweite Methode benutzt lokale Rechnersperren und LVM-"Tags". Diese Methode hat den Vorteil, dass keine LVM-Clusterpakete erforderlich sind. Allerdings sind mehr Schritte zur Einrichtung nötig

und ein Administrator wird nicht daran gehindert, versehentlich einen logischen Datenträger von einem Knoten im Cluster zu entfernen, auf dem es nicht aktiv ist. Das Verfahren zur Konfiguration von HA-LVM mithilfe dieser Methode wird in Abschnitt F.2, „Konfiguration von HA-LVM-Ausfallsicherung mit Tagging“ beschrieben.

F.1. Konfiguration von HA-LVM-Ausfallsicherung mit CLVM (bevorzugt)

Um HA-LVM-Ausfallsicherung (unter Verwendung der bevorzugten CLVM-Variante) einzurichten, führen Sie die folgenden Schritte aus:

1. Vergewissern Sie sich, dass Ihr System zur Unterstützung von CLVM konfiguriert ist. Dazu ist Folgendes erforderlich:
   - Das Hochverfügbarkeits-Add-On und das Resilient Storage Add-On sind installiert, einschließlich des **cmirror** Pakets, falls die CLVM logischen Datenträger gespiegelt werden sollen.
   - Der **locking_type** Parameter im globalen Abschnitt der **/etc/lvm/lvm.conf** Datei ist auf den Wert '3' gesetzt.
   - Die Hochverfügbarkeits-Add-On und Resilient Storage Add-On Software, einschließlich des **clvmd** Daemons, müssen laufen. Für CLVM-Spiegelung muss zudem der **cmirrord** Dienst gestartet sein.
2. Erstellen Sie den logischen Datenträger und das Dateisystem mithilfe der standardmäßigen LVM- und Dateisystem-Befehle, wie im folgenden Beispiel veranschaulicht.

   ```
   # pvcreate /dev/sd[cde]1

   # vgcreate -cy shared_vg /dev/sd[cde]1

   # lvcreate -L 10G -n ha_lv shared_vg

   # mkfs.ext4 /dev/shared_vg/ha_lv

   # lvchange -an shared_vg/ha_lv
   ```

   Informationen über das Anlegen von LVM logischen Datenträgern finden Sie im Handbuch *Administration des Logical Volume Manager*.
3. Bearbeiten Sie die **/etc/cluster/cluster.conf** Datei, um den neu erstellten logischen Datenträger in einem Ihrer Dienste als Ressource hinzuzufügen. Alternativ können Sie **Conga** oder den **ccs** Befehl verwenden, um LVM- und Dateisystem-Ressourcen für den Cluster zu konfigurieren. Nachfolgend sehen Sie einen beispielhaften Ressourcen-Manager Abschnitt aus der **/etc/cluster/cluster.conf** Datei, der einen CLVM logischen Datenträger als Cluster-Ressource konfiguriert:

```
<rm>
   <failoverdomains>
       <failoverdomain name="FD" ordered="1" restricted="0">
          <failoverdomainnode name="neo-01" priority="1"/>
          <failoverdomainnode name="neo-02" priority="2"/>
       </failoverdomain>
   </failoverdomains>
   <resources>
       <lvm name="lvm" vg_name="shared_vg" lv_name="ha-lv"/>
       <fs name="FS" device="/dev/shared_vg/ha-lv" force_fsck="0"
force_unmount="1" fsid="64050" fstype="ext4" mountpoint="/mnt" options=""
self_fence="0"/>
   </resources>
   <service autostart="1" domain="FD" name="serv" recovery="relocate">
       <lvm ref="lvm"/>
       <fs ref="FS"/>
   </service>
</rm>
```

F.2. Konfiguration von HA-LVM-Ausfallsicherung mit Tagging

Um HA-LVM-Ausfallsicherung unter Verwendung von Tags in der **/etc/lvm/lvm.conf** Datei einzurichten, führen Sie die folgenden Schritte aus:

1. Vergewissern Sie sich, dass der **locking_type** Parameter im globalen Abschnitt der **/etc/lvm/lvm.conf** Datei auf den Wert '1' gesetzt ist.
2. Erstellen Sie den logischen Datenträger und das Dateisystem mithilfe der standardmäßigen LVM- und Dateisystem-Befehle, wie im folgenden Beispiel veranschaulicht.

   ```
   # pvcreate /dev/sd[cde]1

   # vgcreate shared_vg /dev/sd[cde]1

   # lvcreate -L 10G -n ha_lv shared_vg

   # mkfs.ext4 /dev/shared_vg/ha_lv
   ```

   Informationen über das Anlegen von LVM logischen Datenträgern finden Sie im Handbuch *Administration des Logical Volume Manager*.
3. Bearbeiten Sie die **/etc/cluster/cluster.conf** Datei, um den neu erstellten logischen Datenträger in einem Ihrer Dienste als Ressource hinzuzufügen. Alternativ können Sie **Conga** oder den **ccs** Befehl verwenden, um LVM- und Dateisystem-Ressourcen für den Cluster zu konfigurieren. Nachfolgend sehen Sie einen beispielhaften Ressourcen-Manager Abschnitt aus der **/etc/cluster/cluster.conf** Datei, der einen CLVM logischen Datenträger als Cluster-Ressource konfiguriert:

```
<rm>
   <failoverdomains>
       <failoverdomain name="FD" ordered="1" restricted="0">
          <failoverdomainnode name="neo-01" priority="1"/>
          <failoverdomainnode name="neo-02" priority="2"/>
       </failoverdomain>
   </failoverdomains>
   <resources>
       <lvm name="lvm" vg_name="shared_vg" lv_name="ha_lv"/>
       <fs name="FS" device="/dev/shared_vg/ha_lv" force_fsck="0"
force_unmount="1" fsid="64050" fstype="ext4" mountpoint="/mnt" options=""
self_fence="0"/>
   </resources>
   <service autostart="1" domain="FD" name="serv" recovery="relocate">
       <lvm ref="lvm"/>
       <fs ref="FS"/>
   </service>
</rm>
```



Anmerkung

Falls es mehrere logische Datenträger in der Datenträgergruppe gibt, sollte der Name des logischen Datenträgers (**`lv_name`**) in der **`lvm`** Ressource leer bleiben oder nicht spezifiziert werden. Beachten Sie außerdem, dass eine Datenträgergruppe in einer HA-LVM-Konfiguration nur von einem einzigen Dienst verwendet werden darf.

4. Bearbeiten Sie das **`volume_list`** Feld in der **`/etc/lvm/lvm.conf`** Datei. Fügen Sie den Namen Ihrer Basis-Datenträgergruppe und Ihren Hostnamen gemäß **`/etc/cluster/cluster.conf`** Datei mit vorangestelltem @ ein. Der Hostname, den Sie hier einfügen, ist der Hostname des Rechners, auf dem Sie die **`lvm.conf`** Datei bearbeiten, kein externer Hostname. Beachten Sie, dass diese Zeichenkette mit dem Knotennamen übereinstimmen *MUSS*, der in der **`cluster.conf`** Datei angegeben ist. Sehen Sie nachfolgend einen Beispieleintrag für die **`/etc/lvm/lvm.conf`** Datei:

   ```
   volume_list = [ "VolGroup00", "@neo-01" ]
   ```

   Dieser Tag wird verwendet, um gemeinsam verwendete Datenträgergruppen oder logische Datenträger zu aktivieren. Fügen Sie *KEINE* Namen von Datenträgergruppen ein, die mittels HA-LVM gemeinsam verwendet werden sollen.

5. Aktivieren Sie das **`initrd`** Gerät auf allen Ihren Cluster-Knoten:

   ```
   # dracut -H -f /boot/initramfs-$(uname -r).img $(uname -r)
   ```

6. Starten Sie alle Knoten neu, um sicherzustellen, dass das korrekte **`initrd`** Gerät verwendet wird.

Versionsgeschichte

Version 6.0-21.2	Thu Feb 27 2014	Hedda Peters

de-DE Übersetzung fertiggestellt

Version 6.0-21.1	Thu Feb 27 2014	Hedda Peters

Übersetzungsdateien synchronisiert mit XML-Quellen 6.0-21

Version 6.0-21	Wed Nov 13 2013	Steven Levine

Version für 6.5 GA-Release

Version 6.0-20	Wed Nov 6 2013	Steven Levine

Behebt: #986462
Aktualisiert die oracledb-Ressourcentabelle.

Version 6.0-16	Tue Oct 29 2013	Steven Levine

Behebt: #1021045
Korrigiert das Beispiel der iptables-Regel.

Version 6.0-15	Fri Sep 27 2013	Steven Levine

Version für 6.5 Beta-Release

Version 6.0-12	Thu Sep 26 2013	Steven Levine

Behebt: #884758, #893575, #969525, #969139, #987151, #987623
Kleinere Aktualisierungen an den Tabellen mit Fencing-Geräteparametern.

Behebt: #901637, #983739, 986462
Kleinere Aktualisierungen an den Tabellen mit Ressourcenparametern.

Behebt: #633495
Dokumentiert die Konfiguration von **`nfsexport`** und **`nfsserver`** Ressourcen.

Behebt: #852966, #975512, #977194, #991297, #874211, #908328, #919600,#955405, #972521, #986474, #987135, #698454, #967986
Kleinere Fehlerkorrekturen und Verdeutlichungen im gesamten Dokument.

Version 6.0-3	Thu Sep 05 2013	Steven Levine

Grundlegende Überarbeitung für alle 6.5 BZs.

Version 6.0-2	Fri Jun 14 2013	Steven Levine

Abschnitt über Konfiguration von nfsserver und nfsexport hinzugefügt.

Version 6.0-1	Thu Jun 13 2013	Steven Levine

Verfahren zur Cluster-Aktualisierung und qdisk-Überlegungen aktualisiert.

Version 5.0-25	Mon Feb 18 2013	Steven Levine

Version für 6.4 GA-Release

Version 5.0-23	Wed Jan 30 2013	Steven Levine

Behebt: 901641
Korrigiert und klärt iptables-Regeln.

Version 5.0-22	Tue Jan 29 2013	Steven Levine

Behebt: 788636
Dokumentiert RRP-Konfiguration durch den **ccs** Befehl.

Behebt: 789010
Dokumentiert RRP-Konfiguration in der **cluster.conf** Datei.

Version 5.0-20	**Fri Jan 18 2013**	**Steven Levine**

Behebt: 894097
Entfernt den Ratschlag sicherzustellen, dass Sie nicht VLAN-Kennzeichnung verwenden.

Behebt: 845365
Zeigt an, dass Bonding-Modus 0 und 2 nun unterstützt werden.

Version 5.0-19	**Thu Jan 17 2013**	**Steven Levine**

Behebt: 896234
Verdeutlicht Terminologie der Cluster-Knoten-Referenzen.

Version 5.0-16	**Mon Nov 26 2012**	**Steven Levine**

Version für 6.4 Beta Release

Version 5.0-15	**Wed Nov 20 2012**	**Steven Levine**

Behebt: 838988
Dokumentiert nfsrestart-Parameter für Dateisystem-Ressourcen-Agenten.

Behebt: 843169
Dokumentiert den IBM iPDU Fencing-Agent.

Behebt: 846121
Dokumentiert den Eaton Network Power Controller (SNMP Schnittstelle) Fencing-Agent.

Behebt: 856834
Dokumentiert den HP BladeSystem Fencing-Agent.

Behebt: 865313
Dokumentiert den NFS-Server Ressourcen-Agenten.

Behebt: 862281
Verdeutlicht, welche **ccs** Befehle die vorherigen Einstellungen überschreiben.

Behebt: 846205
Dokumentiert **iptables** Firewall Filterung für die **igmp** Komponente.

Behebt: 857172
Dokumentiert die Möglichkeit, Benutzer von luci zu entfernen.

Behebt: 857165
Dokumentiert den Berechtigungsebenen-Parameter des IPMI Fencing-Agenten.

Behebt: 840912
Bereinigt Formatierungsproblem in der Ressourcenparameter-Tabelle.

Behebt: 849240, 870292
Verdeutlicht den Installationsablauf.

Behebt: 871165
Verdeutlicht die Beschreibung des IP-Adress-Parameters in der Beschreibung der IP-Adress-Ressourcen-Agenten.

Behebt: 845333, 869039, 856681
Behebt kleine Tippfehler und verdeutlicht kleine technische Unklarheiten.

Version 5.0-12	**Thu Nov 1 2012**	**Steven Levine**

Neu unterstützte Fencing-Agenten hinzugefügt.

Version 5.0-7	**Thu Oct 25 2012**	**Steven Levine**

Abschnitt über Überschreibungsregeln hinzugefügt.

Version 5.0-6	**Tue Oct 23 2012**	**Steven Levine**

Standardwert von Post Join Delay korrigiert.

Version 5.0-4	**Tue Oct 16 2012**	**Steven Levine**

Beschreibung der NFS-Server-Ressource hinzugefügt.

Version 5.0-2	**Thu Oct 11 2012**	**Steven Levine**

Conga-Beschreibungen aktualisiert.

Version 5.0-1	**Mon Oct 8 2012**	**Steven Levine**

ccs-Inhalte verdeutlicht

Version 4.0-5	**Fri Jun 15 2012**	**Steven Levine**

Version für 6.3 GA-Release

Version 4.0-4	**Tue Jun 12 2012**	**Steven Levine**

Behebt: #830148
Gewährleistet die Konsistenz von Portnummer-Beispielen für Luci.

Version 4.0-3	**Tue May 21 2012**	**Steven Levine**

Behebt: #696897
Fügt cluster.conf-Parameterinformationen zu den Tabellen der Fencing-Geräteparameter und Ressourcenparameter hinzu.

Behebt: #811643
Fügt Verfahren zum Wiederherstellen einer **luci** Datenbank auf einem separaten Rechner hinzu.

Version 4.0-2	**Wed Apr 25 2012**	**Steven Levine**

Behebt: #815619
Entfernt Warnung zur Verwendung von UDP Unicast mit GFS2-Dateisystemen.

Version 4.0-1	**Fri Mar 30 2012**	**Steven Levine**

Behebt: #771447, #800069, #800061
Aktualisiert Dokumentation von **luci** zwecks Übereinstimmung mit Red Hat Enterprise Linux 6.3 Version.

Behebt: #712393
Fügt Informationen über das Erstellen eines Speicherauszugs einer Applikation für RGManager hinzu.

Behebt: #800074
Dokumentiert den **condor** Ressourcen-Agent.

Behebt: #757904
Dokumentiert die Sicherung und Wiederherstellung der **luci** Konfiguration.

Behebt: #772374
Fügt einen Abschnitt über die Verwaltung virtueller Maschinen in einem Cluster hinzu.

Behebt: #712378
Fügt Dokumentation für HA-LVM-Konfiguration hinzu.

Behebt: #712400
Dokumentiert Debug-Optionen.

Behebt: #751156
Dokumentiert neue **`fence_ipmilan`** Parameter.

Behebt: #721373
Dokumentiert, welche Konfigurationsänderungen einen Cluster-Neustart erfordern.

Version 3.0-5	**Thu Dec 1 2011**	**Steven Levine**

Release für GA von Red Hat Enterprise Linux 6.2

Behebt: #755849
Korrigiert monitor_link-Parameterbeispiel.

Version 3.0-4	**Mon Nov 7 2011**	**Steven Levine**

Behebt: #755849
Fügt Dokumentation für RHEV-M REST API Fencing-Gerät hinzu.

Version 3.0-3	**Fri Oct 21 2011**	**Steven Levine**

Behebt: #747181, #747182, #747184, #747185, #747186, #747187, #747188, #747189, #747190, #747192
Korrigiert Tippfehler und nicht eindeutige Abschnitte, die während der Qualitätsprüfung der Dokumentation für Red Hat Enterprise Linux 6.2 gefunden wurden.

Version 3.0-2	**Fri Oct 7 2011**	**Steven Levine**

Behebt: #743757
Korrigiert Hinweise auf unterstützten Bonding-Modus im Abschnitt zur Suche und Bereinigung von Fehlern.

Version 3.0-1	**Wed Sep 28 2011**	**Steven Levine**

Erste Revision für Red Hat Enterprise Linux 6.2 Beta Release

Behebt: #739613
Dokumentiert Unterstützung für neue **`ccs`** Optionen, um verfügbare Fencing-Geräte und verfügbare Dienste anzuzeigen.

Behebt: #707740
Dokumentiert Aktualisierungen der Conga-Benutzeroberfläche und dokumentiert Unterstützung des Erstellens von Benutzerberechtigungen zur Verwaltung von Conga.

Behebt: #731856
Dokumentiert die Unterstützung der Konfiguration von **luci** mithilfe der **`/etc/sysconfig/luci`** Datei.

Behebt: #736134
Dokumentiert Unterstützung für UDPU-Transport.

Behebt: #736143
Dokumentiert Unterstützung für geclustertes Samba.

Behebt: #617634
Dokumentiert, wie eine bestimmte IP-Adresse konfiguriert wird, auf der **luci** bereitgestellt werden soll.

Behebt: #713259
Dokumentiert die Unterstützung für den **`fence_vmware_soap`** Agent.

Behebt: #721009
Fügt Link zum Support-Essentials-Artikel hinzu.

Behebt: #717006
Fügt Informationen über das Zulassen von Multicast-Datenverkehr durch die **`iptables`** Firewall hinzu.

Behebt: #717008
Fügt Informationen über die Statusprüfung von Cluster-Diensten und über die Zeitüberschreitung der Ausfallsicherung hinzu.

Behebt: #711868
Verdeutlicht die Beschreibung der autostart-Option.

Behebt: #728337
Dokumentiert das Verfahren zum Hinzufügen einer **`vm`** Ressource mithilfe des **`ccs`** Befehls.

Behebt: #725315, #733011, #733074, #733689
Korrigiert kleinere Tippfehler.

Version 2.0-1	**Thu May 19 2011**	**Steven Levine**

Erste Revision für Red Hat Enterprise Linux 6.1

Behebt: #671250
Dokumentiert Unterstützung für SNMP-Traps.

Behebt: #659753
Dokumentiert den **`ccs`** Befehl.

Behebt: #665055
Aktualisiert Conga-Dokumentation mit aktualisierter Anzeige und unterstützten Features.

Behebt: #680294
Dokumentiert die Notwendigkeit des Passwortzugriffs für **`ricci`** Agent.

Behebt: #687871
Fügt Kapitel zur Suche und Bereinigung von Fehlern hinzu.

Behebt: #673217
Behebt Tippfehler.

Behebt: #675805
Fügt Hinweis auf **`cluster.conf`** Schema zu Tabellen der Hochverfügbarkeitsressourcen-Parameter hinzu.

Behebt: #672697
Aktualisiert Tabellen der Fencing-Geräteparameter, um alle derzeit unterstützten Fencing-Geräte einzubeziehen.

Behebt: #677994
Korrigiert Informationen für **`fence_ilo`** Fencing-Agentenparameter.

Behebt: #629471
Fügt technischen Hinweis über das Erstellen des consensus-Werts in einem Zwei-Knoten-Cluster hinzu.

Behebt: #579585
Aktualisiert Abschnitt über das Aktualisieren der Red Hat Hochverfügbarkeits-Add-On-Software.

Behebt: #643216
Verdeutlicht einige Sachverhalte im gesamten Dokument.

Behebt: #643191
Verbessert und korrigiert die **luci**> Dokumentation.

Behebt: #704539
Aktualisiert die Parametertabelle für virtuellen Maschinen-Ressourcen.

Version 1.0-1	**Wed Nov 10 2010**	**Paul Kennedy**

Erste Release für Red Hat Enterprise Linux 6

Stichwortverzeichnis

A

ACPI
- Konfiguration, Konfiguration von ACPI zur Verwendung mit integrierten Fencing-Geräten

allgemein
- Überlegungen zur Cluster-Administration, Allgemeine Überlegungen zur Konfiguration

Arten
- Cluster-Ressource, Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten

Ausfallsicherung, Zeitüberschreitung, Prüfung der Cluster-Dienstressource und Zeitüberschreitung der Ausfallsicherung

B

Brocade Fabric Switch Fencing-Gerät, Parameter der Fencing-Geräte

C

CISCO MDS Fencing-Gerät, Parameter der Fencing-Geräte

Cisco UCS Fencing-Gerät, Parameter der Fencing-Geräte

Cluster
- Administration, Vor der Konfiguration des Hochverfügbarkeits-Add-Ons, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Conga, Verwaltung des Red Hat

Hochverfügbarkeits-Add-Ons mit ccs, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools
- Fehlerdiagnose und -behebung, Fehlerdiagnose und -behebung in einem Cluster, Fehlerdiagnose und -behebung in einem Cluster
- Starten, Stoppen und Neustarten, Starten und Stoppen der Cluster-Software

Cluster-Administration, Vor der Konfiguration des Hochverfügbarkeits-Add-Ons, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Conga, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit ccs, Verwaltung des Red Hat Hochverfügbarkeits-Add-Ons mit Befehlszeilen-Tools
- Aktivieren von IP-Ports, Aktivieren von IP-Ports
- Aktualisieren der Cluster-Konfiguration mittels cman_tool version -r, Aktualisieren der Konfiguration mittels cman_tool version -r
- Aktualisieren der Cluster-Konfiguration mittels scp, Aktualisieren der Konfiguration mittels scp
- Aktualisieren einer Konfiguration, Aktualisieren einer Konfiguration
- Allgemeine Überlegungen, Allgemeine Überlegungen zur Konfiguration
- Anzeige von Hochverfügbarkeitsdiensten mit clustat, Anzeige des Hochverfügbarkeitsdienst-Status mit clustat
- Cluster-Knoten entfernen, Ein Mitglied aus einem Cluster löschen
- Cluster-Knoten hinzufügen, Ein Mitglied zu einem laufenden Cluster hinzufügen, Ein Mitglied zu einem laufenden Cluster hinzufügen
- Cluster-Knoten neu starten, Einen Cluster-Knoten neu starten
- Einem Cluster beitreten, Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen, Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen
- Einen Cluster verlassen, Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen, Einen Knoten zum Verlassen oder Beitreten eines Clusters veranlassen
- Einen Knoten aus der Konfiguration löschen; Einen Knoten zur Konfiguration hinzufügen, Hinzufügen oder Löschen eines Knotens
- Fehlerdiagnose und -behebung in einem Cluster, Fehlerdiagnose und -behebung in einem Cluster, Fehlerdiagnose und -behebung in einem Cluster
- kompatible Hardware, Kompatible Hardware
- Konfiguration iptables, Aktivieren von IP-Ports
- Konfiguration von ACPI, Konfiguration von ACPI zur Verwendung mit integrierten Fencing-Geräten
- Löschen eines Clusters, Starten, Stoppen, Neustarten und Löschen von Clustern
- NetworkManager, Überlegungen zum NetworkManager
- Netzwerk-Switches und Multicast-Adressen, Multicast-Adressen
- Neustarten eines Clusters, Starten, Stoppen, Neustarten und Löschen von Clustern
- ricci Überlegungen, Überlegungen zu ricci
- SELinux, Red Hat Hochverfügbarkeits-Add-On und SELinux
- Starten eines Clusters, Starten, Stoppen, Neustarten und Löschen von Clustern, Starten und Stoppen eines Clusters
- Starten, Stoppen und Neustarten eines Clusters, Starten und Stoppen der Cluster-Software
- Stoppen eines Clusters, Starten, Stoppen, Neustarten und Löschen von Clustern, Starten und Stoppen eines Clusters
- Überlegungen zur Verwendung von qdisk, Überlegungen zur Verwendung von Quorum Disk
- Überlegungen zur Verwendung von Quorum Disk, Überlegungen zur Verwendung von Quorum Disk
- Überprüfung der Konfiguration, Überprüfung der Konfiguration
- Verwaltung von Cluster-Knoten, Verwaltung von Cluster-Knoten, Verwaltung von Cluster-Knoten
- Verwaltung von Hochverfügbarkeitsdiensten, Verwaltung von Hochverfügbarkeitsdiensten, Verwaltung von Hochverfügbarkeitsdiensten
- Verwaltung von Hochverfügbarkeitsdiensten, freeze und unfreeze, Verwaltung von

Hochverfügbarkeitsdiensten mit clusvcadm, Überlegungen zur Verwendung der Freeze- und Unfreeze-Operationen
- Virtuelle Maschinen, Konfiguration von virtuellen Maschinen in einer Cluster-Umgebung

Cluster-Dienst-Verwaltung
- Konfiguration, Hinzufügen eines Cluster-Dienstes zum Cluster, Hinzufügen eines Cluster-Dienstes zum Cluster, Hinzufügen eines Cluster-Dienstes zum Cluster

Cluster-Dienste, Hinzufügen eines Cluster-Dienstes zum Cluster, Hinzufügen eines Cluster-Dienstes zum Cluster, Hinzufügen eines Cluster-Dienstes zum Cluster
- (Siehe auch zur Cluster-Konfiguration hinzufügen)

Cluster-Konfiguration, Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Conga, Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit dem ccs Befehl, Manuelle Konfiguration von Red Hat Hochverfügbarkeit
- aktualisieren, Aktualisieren einer Konfiguration
- Hinzufügen oder Löschen eines Knotens, Hinzufügen oder Löschen eines Knotens

Cluster-Ressource, Statusprüfung, Prüfung der Cluster-Dienstressource und Zeitüberschreitung der Ausfallsicherung

Cluster-Ressourcenarten, Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten

Cluster-Ressourcenrelationen, Eltern-, Kind- und Geschwisterrelationen zwischen den Ressourcen

Cluster-Software
- Konfiguration, Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit Conga, Konfiguration des Red Hat Hochverfügbarkeits-Add-Ons mit dem ccs Befehl, Manuelle Konfiguration von Red Hat Hochverfügbarkeit

Conga
- Zugriff, Konfiguration der Red Hat Hochverfügbarkeits-Add-On-Software

consensus-Wert, Der consensus Wert für totem in einen Zwei-Knoten-Cluster

D

Dell DRAC 5 Fencing-Gerät, Parameter der Fencing-Geräte

Dell iDRAC Fencing-Gerät, Parameter der Fencing-Geräte

E

Eaton Network Power Switch, Parameter der Fencing-Geräte

Egenera SAN-Controller Fencing-Gerät, Parameter der Fencing-Geräte

Einführung, Einführung
- weitere Red Hat Enterprise Linux Dokumente, Einführung

ePowerSwitch Fencing-Gerät, Parameter der Fencing-Geräte

F

Feedback, Feedback

fence agent
- fence_eaton_snmp, Parameter der Fencing-Geräte
- fence_hpblade, Parameter der Fencing-Geräte
- fence_ipdu, Parameter der Fencing-Geräte

Fence virt Fencing-Gerät, Parameter der Fencing-Geräte

fence_apc Fencing-Agent, Parameter der Fencing-Geräte

fence_apc_snmp Fencing-Agent, Parameter der Fencing-Geräte

fence_bladecenter Fencing-Agent, Parameter der Fencing-Geräte

fence_brocade Fencing-Agent, Parameter der Fencing-Geräte

fence_cisco_mds Fencing-Agent, Parameter der Fencing-Geräte

fence_cisco_ucs Fencing-Agent, Parameter der Fencing-Geräte

fence_drac5 Fencing-Agent, Parameter der Fencing-Geräte

fence_eaton_snmp fence agent, Parameter der Fencing-Geräte

fence_egenera Fencing-Agent, Parameter der Fencing-Geräte

fence_eps Fencing-Agent, Parameter der Fencing-Geräte

fence_hpblade fence agent, Parameter der Fencing-Geräte

fence_ibmblade Fencing-Agent, Parameter der Fencing-Geräte

fence_idrac Fencing-Agent, Parameter der Fencing-Geräte

fence_ifmib Fencing-Agent, Parameter der Fencing-Geräte

fence_ilo Fencing-Agent, Parameter der Fencing-Geräte

fence_ilo2 Fencing-Agent, Parameter der Fencing-Geräte

fence_ilo3 Fencing-Agent, Parameter der Fencing-Geräte

fence_ilo4 Fencing-Agent, Parameter der Fencing-Geräte

fence_ilo_mp Fencing-Agent, Parameter der Fencing-Geräte

fence_imm Fencing-Agent, Parameter der Fencing-Geräte

fence_intelmodular Fencing-Agent, Parameter der Fencing-Geräte

fence_ipdu fence agent, Parameter der Fencing-Geräte

fence_ipmilan Fencing-Agent, Parameter der Fencing-Geräte

fence_rhevm Fencing-Agent, Parameter der Fencing-Geräte

fence_rsb Fencing-Agent, Parameter der Fencing-Geräte

fence_scsi Fencing-Agent, Parameter der Fencing-Geräte

fence_virt Fencing-Agent, Parameter der Fencing-Geräte

fence_vmware_soap Fencing-Agent, Parameter der Fencing-Geräte

fence_wti Fencing-Agent, Parameter der Fencing-Geräte

Fencing-Agent
- fence_apc, Parameter der Fencing-Geräte
- fence_apc_snmp, Parameter der Fencing-Geräte
- fence_bladecenter, Parameter der Fencing-Geräte
- fence_brocade, Parameter der Fencing-Geräte
- fence_cisco_mds, Parameter der Fencing-Geräte
- fence_cisco_ucs, Parameter der Fencing-Geräte
- fence_drac5, Parameter der Fencing-Geräte
- fence_egenera, Parameter der Fencing-Geräte

- fence_eps, Parameter der Fencing-Geräte
- fence_ibmblade, Parameter der Fencing-Geräte
- fence_idrac, Parameter der Fencing-Geräte
- fence_ifmib, Parameter der Fencing-Geräte
- fence_ilo, Parameter der Fencing-Geräte
- fence_ilo2, Parameter der Fencing-Geräte
- fence_ilo3, Parameter der Fencing-Geräte
- fence_ilo4, Parameter der Fencing-Geräte
- fence_ilo_mp, Parameter der Fencing-Geräte
- fence_imm, Parameter der Fencing-Geräte
- fence_intelmodular, Parameter der Fencing-Geräte
- fence_ipmilan, Parameter der Fencing-Geräte
- fence_rhevm, Parameter der Fencing-Geräte
- fence_rsb, Parameter der Fencing-Geräte
- fence_scsi, Parameter der Fencing-Geräte
- fence_virt, Parameter der Fencing-Geräte
- fence_vmware_soap, Parameter der Fencing-Geräte
- fence_wti, Parameter der Fencing-Geräte

Fencing-Gerät
- APC Power Switch über SNMP, Parameter der Fencing-Geräte
- APC Power Switch über Telnet/SSH, Parameter der Fencing-Geräte
- Brocade Fabric Switch, Parameter der Fencing-Geräte
- Cisco MDS, Parameter der Fencing-Geräte
- Cisco UCS, Parameter der Fencing-Geräte
- Dell DRAC 5, Parameter der Fencing-Geräte
- Dell iDRAC, Parameter der Fencing-Geräte
- Eaton Network Power Switch, Parameter der Fencing-Geräte
- Egenera SAN-Controller, Parameter der Fencing-Geräte
- ePowerSwitch, Parameter der Fencing-Geräte
- Fence virt, Parameter der Fencing-Geräte
- Fujitsu Siemens Remoteview Service Board (RSB), Parameter der Fencing-Geräte
- HP BladeSystem, Parameter der Fencing-Geräte
- HP iLO, Parameter der Fencing-Geräte
- HP iLO MP, Parameter der Fencing-Geräte
- HP iLO2, Parameter der Fencing-Geräte
- HP iLO3, Parameter der Fencing-Geräte
- HP iLO4, Parameter der Fencing-Geräte
- IBM BladeCenter, Parameter der Fencing-Geräte
- IBM BladeCenter SNMP, Parameter der Fencing-Geräte
- IBM Integriertes Managementmodul, Parameter der Fencing-Geräte
- IBM iPDU, Parameter der Fencing-Geräte
- IF MIB, Parameter der Fencing-Geräte
- Intel Modular, Parameter der Fencing-Geräte
- IPMI LAN, Parameter der Fencing-Geräte
- RHEV-M REST API, Parameter der Fencing-Geräte
- SCSI-Fencing, Parameter der Fencing-Geräte
- VMware (SOAP-Schnittstelle), Parameter der Fencing-Geräte
- WTI Power Switch, Parameter der Fencing-Geräte

Fencing-Gerät APC Power Switch über SNMP, Parameter der Fencing-Geräte

Fencing-Gerät APC Power Switch über Telnet/SSH, Parameter der Fencing-Geräte

Fujitsu Siemens Remoteview Service Board (RSB) Fencing-Gerät, Parameter der Fencing-Geräte

H

Hardware
- kompatibel, Kompatible Hardware

Hochverfügbarkeitsdienst, Konfiguration
- Überblick, Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten

HP Bladesystem Fencing-Gerät, Parameter der Fencing-Geräte

HP iLO Fencing-Gerät, Parameter der Fencing-Geräte

HP iLO MP Fencing-Gerät, Parameter der Fencing-Geräte

HP iLO2 Fencing-Gerät, Parameter der Fencing-Geräte

HP iLO3 Fencing-Gerät, Parameter der Fencing-Geräte

HP iLO4 Fencing-Gerät, Parameter der Fencing-Geräte

I

IBM BladeCenter Fencing-Gerät, Parameter der Fencing-Geräte

IBM BladeCenter SNMP Fencing-Gerät, Parameter der Fencing-Geräte

IBM Integriertes Managementmodul Fencing-Gerät, Parameter der Fencing-Geräte

IBM iPDU Fencing-Gerät, Parameter der Fencing-Geräte

IF MIB Fencing-Gerät, Parameter der Fencing-Geräte

integrierte Fencing-Geräte
- Konfiguration von ACPI, Konfiguration von ACPI zur Verwendung mit integrierten Fencing-Geräten

Intel Modular Fencing-Gerät, Parameter der Fencing-Geräte

IP-Ports
- aktivieren, Aktivieren von IP-Ports

IPMI LAN Fencing-Gerät, Parameter der Fencing-Geräte

iptables
- Konfiguration, Aktivieren von IP-Ports

iptables-Firewall, Konfiguration der iptables-Firewall zum Erlauben von Cluster-Komponenten

K

Konfiguration
- Hochverfügbarkeitsdienst, Überlegungen zur Konfiguration von Hochverfügbarkeitsdiensten

Konfiguration von High Availability LVM, High Availability LVM (HA-LVM)

L

LVM, High Availability, High Availability LVM (HA-LVM)

M

Multicast-Adressen
- Überlegungen zur Verwendung mit Netzwerk-Switches und Multicast-Adressen, Multicast-Adressen

Multicast-Datenverkehr aktivieren, Konfiguration der iptables-Firewall zum Erlauben von Cluster-Komponenten

N

NetworkManager
- deaktivieren beim Einsatz eines Clusters, Überlegungen zum NetworkManager

Neue und veränderte Features, Neue und veränderte Features

nfsexport-Ressource, Konfiguration, Konfiguration von nfsexport- und nfsserver-Ressourcen

nfsserver-Ressource, Konfiguration, Konfiguration von nfsexport- und nfsserver-Ressourcen

P

Parameter, Fencing-Gerät, Parameter der Fencing-Geräte

Parameter, Hochverfügbarkeitsressourcen, Parameter der Hochverfügbarkeitsressourcen

Q

qdisk
- Überlegungen zur Verwendung, Überlegungen zur Verwendung von Quorum Disk

Quorum Disk
- Überlegungen zur Verwendung, Überlegungen zur Verwendung von Quorum Disk

R

Relationen
- Cluster-Ressource, Eltern-, Kind- und Geschwisterrelationen zwischen den Ressourcen

RHEV-M REST API Fencing-Gerät, Parameter der Fencing-Geräte

ricci
- Überlegungen zur Cluster-Administration, Überlegungen zu ricci

S

SCSI-Fencing, Parameter der Fencing-Geräte

SELinux
- Konfiguration, Red Hat Hochverfügbarkeits-Add-On und SELinux

Statusprüfung, Cluster-Ressource, Prüfung der Cluster-Dienstressource und

Zeitüberschreitung der Ausfallsicherung

Suche und Beseitigung von Fehlern
- Fehlerdiagnose und -behebung in einem Cluster, Fehlerdiagnose und -behebung in einem Cluster, Fehlerdiagnose und -behebung in einem Cluster

T

Tabellen
- Fencing-Geräte, Parameter, Parameter der Fencing-Geräte
- Hochverfügbarkeitsressourcen, Parameter, Parameter der Hochverfügbarkeitsressourcen

Tools, Befehlszeile, Überblick über Befehlszeilen-Tools

Totem-Tag
- consensus-Wert, Der consensus Wert für totem in einen Zwei-Knoten-Cluster

U

Überblick
- Neue und veränderte Features, Neue und veränderte Features

Überprüfung
- Cluster-Konfiguration, Überprüfung der Konfiguration

V

Verhalten, Hochverfügbarkeitsressourcen, Verhalten der Hochverfügbarkeitsressourcen

Virtuelle Maschinen in einem Cluster, Konfiguration von virtuellen Maschinen in einer Cluster-Umgebung

VMware (SOAP-Schnittstelle) Fencing-Gerät, Parameter der Fencing-Geräte

W

WTI Power Switch Fencing-Gerät, Parameter der Fencing-Geräte

Z

Zeitüberschreitung, Ausfallsicherung, Prüfung der Cluster-Dienstressource und Zeitüberschreitung der Ausfallsicherung